BTX-4K APPLICATION MANUAL

Release 2.2

299-432-505

NUERA™

First Edition (February 2007)

This edition applies to the Nuera Communications, Inc. BTX-4K gateway. The licensed product described in this document and all licensed materials that are available for it are provided by Nuera under terms of the agreement for Nuera licensed products. Nuera periodically makes additions, deletions, or changes to the information in this document. Before you use this document, consult Nuera or your distributor for the most recent Nuera edition.

The author and publisher have made reasonable efforts to ensure the accuracy and timeliness of the information in this book. However, neither the author nor the publisher shall have any liability with respect to loss or damage caused or alleged to be caused by reliance on any information in this book.

Nuera may have patents or pending patent applications covering material in this document. Furnishing this document does not of itself constitute a grant of any license or immunity under any patents, patent applications, trademarks, copyrights, or other rights of Nuera, or of any third party, or any right to refer to Nuera in any advertising or other marketing activities. Nuera assumes no responsibility for any infringement of patents or other rights of third parties that may result from use of the material in this document or for the manufacture, use, lease, or sale of machines or software programs described herein, outside of any responsibilities assumed in the original or subsequent purchase or lease agreements.

This document may contain information about, or make reference to, Nuera products, programming, or services that are not available in your country. This information must not be construed to mean that Nuera intends to make available such products, programs, or services in your country.

A form for your comments is provided at the back of this document. If the form has been removed, address your comments to: Nuera Communications, Inc., Professional Services, 9890 Towne Center Drive, Suite 150, San Diego, CA 92121.

Nuera may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

No part of this publication may be reproduced in any manner without the written permission of Nuera, Inc. For information, write to: Nuera Communications, Inc., Legal Office, 9890 Towne Center Drive, Suite 150, San Diego, CA 92121.

© 2007 by Nuera Communications, Inc.

All rights reserved

Warranty

Nuera's standard warranty is one year from the date of shipment and is verified by serial number of the system. Any defective component will be replaced or repaired at no charge during this period. If any equipment fails within the first 90 days of shipment, an advance replacement will be sent or on-site repair performed at Nuera's discretion, at no charge. After that period, and for the reminder of the warranty, defective modules will be repaired at Nuera and then returned to the customer.

Once the warranty has expired, the components can either be returned to Nuera for repair, or an advance replacement can be provided. The repair and advance replacement pricing are described in the Nuera Global Pricelist.

In order to exercise your rights to repair under this warranty, you must first contact Nuera to obtain a repair authorization (RA) number. If you must return the unit to Nuera for repair while the unit is under warranty, Nuera will pay the cost of shipping it to and from Nuera.

Software License Agreement

Each software Product, including any documentation relating to or describing such Software, provided by Nuera (hereinafter collectively called "Software") is furnished to you under a nonexclusive, nontransferable license solely for your own use only on the single processor on which the Software is first installed. The Software may not be copied, in whole or in part, except for archival purposes, to replace a defective copy, or for program error verification.

You may not reverse engineer, decompile, or disassemble the Software, except to the extent such foregoing restriction is expressly prohibited by applicable law.

The term of each paid-up license shall expire at such time as you discontinue use of the applicable Software on the single processor specified above but otherwise shall be without restriction as to time.

The Software (including any images, applets, photographs, animations, video, audio, music, and text incorporated into the Software) is owned by Nuera or its suppliers and is protected by United States copyright laws and international treaty provisions.

Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either (a) make one copy of the Software solely for backup or archival purposes, or (b) transfer the Software to a single hard disk provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the Software.

ORCA User Library

All books that support the ORCA product line are provided on a compact disc (CD) in Adobe Acrobat format. Included on the CD is the appropriate version of Adobe Acrobat Reader.

This section lists the titles of all the books in the ORCA library. To order any of these books, contact your distributor or Nuera directly. To make comments or suggestions regarding any of these books, direct your correspondence to **tac@nuera.com**.

Number	Book
299-225-4*nn*	***ORCA SSC Softswitch User's Guide***
	This guide presents conceptual information about the use and functionality of the ORCA SSC Softswitch. It also provides information about installing and configuring SSC for use with other equipment.
299-193-5*nn*	***ORCA GX-Series Software Manual***
	This manual is designed for the system integrator/system administrator who needs to configure ORCA GX gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the ORCA GX gateway correctly configured using network management software.
299-297-5*nn*	***ORCA RDT-8g Software Manual***
	This manual is designed for the system integrator/system administrator who needs to configure ORCA RDT-8g gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the ORCA RDT-8g gateway correctly configured using network management software.
299-298-5*nn*	***ORCA RDT-8v Software Manual***
	This manual is designed for the system integrator/system administrator who needs to configure ORCA RDT-8v gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the ORCA RDT-8v gateway correctly configured using network management software.

Number	Book
299-252-5*nn*	***ORCA BTX-Series Software Manual***
	This manual is designed for the system integrator/system administrator who needs to configure ORCA BTX gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the ORCA BTX gateway correctly configured using network management software.
299-335-1*nn*	***ORCA Gateway Hardware Manual***
	This manual presents conceptual information about the use, functionality, and specifications of the ORCA 21-slot and 8-slot gateways, including installation steps and information.
299-433-1*nn*	***ORCA-4K Hardware Manual***
	This manual presents conceptual information about the use, functionality, and specifications of the ORCA 4K gateway, including installation steps and information.
299-432-5*nn*	***ORCA BTX-4K Application Manual***
	This manual is designed for the system integrator/system administrator who needs to configure BTX-4K gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the BTX-4K gateway correctly configured using network management software.
299-442-5*nn*	***ORCA UMX-4K Application Manual***
	This manual is designed for the system integrator/system administrator who needs to configure UMX-4K gateways at an end-user site. Its purpose is to guide this individual through the configuration steps required to get the UMX-4K gateway correctly configured using network management software.
299-434-4*nn*	***NetConductor User's Guide***
	This guide presents conceptual information about the use, functionality, and specifications of the NetConductor application, including installation steps and information.

Additional ORCA books are available in PDF format from Nuera's web site, http://www.nuera.com. For information regarding pricing and availability, contact a sales representative at:

Nuera Communications, Inc.
9890 Towne Center Drive, Suite 150
San Diego, CA 92121
858-625-2400

Trademarks Used in This Manual

The following list contains trademarks that are used in this manual. In the United States, these trademarks are registered trademarks; in World Trade countries, these trademarks are not registered.

Trademark	Trademark Owner
ANSI	American National Standards Institute
Cisco	Cisco Systems, Inc.
IBM	International Business Machines, Inc.
Microsoft	Microsoft Corporation, Inc.
ORCA	Nuera Communications, Inc.
UNIX	The Open Group
VT100	Compaq Digital Equipment Corporation
Windows XP	Microsoft Corporation, Inc.
Red Hat Linux	Red Hat
MySQL	MySQL AB

TABLE OF CONTENTS

About This Book 11
Who Should Use This Book 11
Conventions Used in This Book 11
Notes, Cautions, and Warnings 11
How Numbers Are Used 12
Replaceable Input Values 12
Getting Help 13
Checklist 14
Contacts 14

Chapter 1. Introduction 15
BTX-4K Features 15
Capacity 15
PacketCable TGCP Compliance 16
PacketCable CALEA Compliance 16
PacketCable Security Compliance 16
Multiple MGC Connectivity 17
ISDN Backhaul 17
SNMPv3 17
DNS Lookup 17
Force Connect 17
Voice Codecs 17
Echo Cancellation 18
Voice Activity Detection 18
Lost Packet Recovery / Packet Loss Concealment 18
Inband Signaling, Fax and Modem Support 18
Differentiated Services (Diffserv) 19
TFTP Access List 19
Syslog 19
Physical Connections 19
Typical Network Application Configuration 20
BTX-4K in a PacketCable Network 20
CableLabs Certification 21
BTX-4K in a Force Connect Application 21
Nuera NetConductor 22
NetConductor (EMS) Network Layout 23

SNMPv3. 23

Chapter 2. Getting Started 25
Craft Port 25
IP Address Configuration 26
Physical Connections 27
Accessing NetConductor. 28
The User Interface 28
Links Pane. 29
Navigation Pane 30
Information Pane 30
Alarm Pane 32

Chapter 3. Configuring Resources. 35
Prerequisites 35
Initial Configuration. 36
Adding a Network Element 36
Configuring the BITS Clock 38
Configuring NetRef. 39
Configuring DNS. 41
Configuring IPsec 42
Configuring Media Gateway Controllers for TGCP Applications . . . 44
Configuring Remote Gateways for Force Connect Applications 47
Configuring TDM Interfaces 50
Configuring DS1 and E1 Parameters 68
Configuring Network Globals. 78
Configuring TrapTargets 79
Configuring TFTP Clients 80
Configuring System Global Parameters 81
Configuring Hardware Settings. 83
Configuring IUA 84

Chapter 4. Viewing System Status 95
Introduction 95
Repolling the System 96
Refresh Link 96
Monitoring using NetConductor Logs 97
Hardware Options and Statistics 97
VPM Status 97
BCM Status 103
OCMCard Status 105
OC3DB Card Status 107
DS3DB Card Status 108
DSP Status 110
NP Status 113
Fan Status 115
DS3X Status 117
Sensor Status 118

ALARM Status 120
Interface Parameters and Statistics 121
Ethernet Status. 121
DoS Statistics 124
BITS Status. 126
DS3 Status 128
OC3 Status 133
OC3 Working and Protect Interface Status 137
STS1 Status. 141
DS1 and E1 Status 145
STM-1 Status 150
STM-1 Working and Protect Interface Status. 153
VC4 Status 156
DS0 Status 159
IPSec Template Status 165
DNS Server Status 166
DNS Resolver Status 168
NETREF Globals Status 169
Signaling Backhaul Parameters and Stats 170
SCTP Globals Status 170
ASPGroup Status 177
ASP Status 178
Backhaul Trunk Status 183
System Globals Status 187

Chapter 5. Managing The Gateway 190
Using Syslog 190
Configuring Debug classes 193
Upgrading the Firmware 198
Upgrading Capacity and Vocoder Capability 201
Maintenance Procedures 202
Forcing a Switchover 202
Version Information 203

Chapter 6. Troubleshooting 204
Connection Issues 204
IP Address Conflicts 204
License Upgrade Issues 204
Symptoms 204
Possible Causes 204
Solutions 205
Firmware Upgrade Issues 205
Symptoms 205
Possible Causes 205
Solutions 205
MO/MT Channel Issues 205
Symptoms – Scenario 1. 205
Possible Causes 206

Solutions 206
Symptoms – Scenario 2. 206
Possible Causes 206
Solutions 206
MG to MGC Communications 206
Symptoms – Scenario 1. 206
Possible Causes 206
Solutions 207
Symptoms – Scenario 2. 207
Possible Causes 207
Solutions 207
Voice Issues 207
Symptoms – Scenario 1. 207
Possible Causes 208
Solutions 208
Symptoms – Scenario 2. 208
Possible Cause. 208
Solution 208
Symptoms - Scenario 3 208
Possible Cause. 208
Solutions 209
Fax/Modem Issues – Packet Loss 209
Symptoms 209
Possible Cause. 209
Solution 209
Fax/Modem Issues – Clocking 209
Symptoms 209
Possible Causes 209
Solutions 209
100 BT Interface Issues 210
Symptoms 210
Possible Causes 210
Solutions 210

Appendix A. Syslog Debug Classes 211
CCP Classes 211
DSP Classes 216
NP Classes 217

Appendix B. OC3 (SONET) DS1 and STM-1 (SDH) VC12/E1 Mapping 218
DS1 to OC3 (SONET) Mapping 219
VC12/E1 to STM-1 (SDH) Mapping. 220

Glossary 221

Bibliography 226
MicroMuse, Inc. 226

About This Book

This book presents the design and operation of the Open Reliable Communications Architecture (ORCA) telephony gateway. Specifically, this book provides information on configuring and maintaining the ORCA BTX-4K gateway.

Who Should Use This Book

This book is for product distributors, systems integrators, systems analysts, and network administrators who design, install, configure, and maintain wide area networks (WANs) and large-scale communications applications. It contains conceptual and practical information about how to use the BTX-4K gateway within your network.

Conventions Used in This Book

This book uses specific conventions to show the following types of information:

- Number usage
- Replaceable input values
- Messages

Read the following sections to learn more about how this information is shown in the rest of the book.

Notes, Cautions, and Warnings

Notes show useful information requiring your attention.

Cautions show information requiring extra attention.

Warnings are information that, if not followed, could result in injury or equipment damage.

How Numbers Are Used

When numbers are shown in this book, they can appear as descriptive values or as data to be manipulated internally. Decimal values are used frequently; however, alternate number bases are useful when internal data is shown.

Large Decimal Numbers

Numbers greater than 9999 display in SI metric style, where whole numbers that contain more than four digits are broken into groups of three digits that are separated by spaces. For example, the number sixteen thousand three hundred eighty three is shown as 16 383. This avoids confusion between American and European punctuation conventions. However, a number that is internally manipulated by a computer is shown without punctuation or spaces. For example, notice how the value 65 535 appears in the following instruction without a space or a thousands separator within the number:

```
Specify 65535 as a maximum value
```

Numbers with Different Bases

All numbers shown in this book are decimal values unless the number base is binary or hexadecimal. In these cases, an identifier precedes a binary or hexadecimal number. For example:

- the value of binary 1010
- the value of hex 4F

Replaceable Input Values

In some cases, you can insert user-defined values into commands or you can specify local paths and filenames. These variable values are shown in *italic* typeface.

For example, you might be asked to specify the name of your server in this path:

A:\LOGIN\LOGIN *servername*

The italic typeface shows that you need to replace *servername* with your local server name.

When you are prompted for variable input that is represented by lower-case letters, follow these conventions:

When You See This	Substitute This Value
b	Any binary digit
h	Any hexadecimal digit
n	Any decimal digit
x	Any alphabetic value, such as: ***x*:\DOS** where you substitute the correct drive letter for *x*
Multiple letters	A series of digits, such as: FIRST 2 HEX BYTES: ***hhhh*** where you substitute four hexadecimal digits for *hhhh*

When you are prompted for variable input with embedded decimal points, replace the variable digits and let the decimal points remain to separate 32-bit dotted-decimal address segments. For example, you might be prompted to supply a 32-bit, dotted-decimal address in this format:

nnn.nnn.nnn.nnn

where ***nnn*** is a decimal value from 0 through 255. Leading zeros are not required.

GETTING HELP

If, after installing and configuring your Nuera equipment, you cannot establish communications to or from the unit, carefully review the information in this book and in the other ORCA books prior to calling Technical Assistance Center (TAC).

Before going any further, check with your System Administrator for proper operation of the server machine, including your Linux operating system, MySQL database, and NetConductor software. It may be necessary to reboot the Linux server.

Checklist

If, after carefully reviewing the information in this book and in the other ORCA books, your problem persists, contact your product representative or a service representative at Nuera's Technical Assistance Center. So we can serve you better, make a list of the following items before calling:

- A detailed description of your problem.
- A complete listing of your system components and configuration, including the serial number of your unit and the software version number it is running.
- A narrative of the actions you performed prior to the problem.
- A list of all system messages posted by your unit.

Contacts

Address:
Nuera Communications, Inc.
9890 Towne Center Drive, Suite 150
San Diego, CA 92121 USA
tac@nuera.com
www.nuera.com/support/

Telephone:
1-858-625-9220, extension 1391
1-800-966-8372, extension 1391

1

INTRODUCTION

The Open Reliable Communications Architecture (ORCA) BTX-4K is designed to bridge the gap between traditional, circuit-based Public Switched Telephone Networks (PSTNs) and emerging, packet-switched telephony networks, such as cable and digital subscriber line (DSL) networks. The BTX-4K uses advanced signal processing techniques to characterize and format signal sources into data packets, making it an excellent solution for merging digital broadband access networks with the legacy telephone network in a seamless, reliable manner.This book contains an overview of features and information on how to set up and maintain a BTX-4K using the Nuera NetConductor Element Management System (EMS).

BTX-4K Features

The BTX-4K supports the following features:

Capacity

Interface	**# of T1/E1**	**DS0 (voice channels)**
6 DS3 (metallic)	168 T1s	4,032
2 OC-3 (optical)	168 T1s	4,032
2 STM-1 (optical)	126 E1s	3,906

Contact Nuera for current capacity increment information.

PacketCable TGCP Compliance

PacketCable defines the PSTN Trunking Gateway Call Signaling Protocol, TGCP 1.0. TGCP is a profile of MGCP derived from MGCP Version 1.0. The profile defines naming conventions, the usage of the session description protocol (SDP), and the procedures that compose TGCP.

The BTX-4K supports IT, ISUP, MO and MT event packages, as well as the T.38 Fax relay and RFC2833 DTMF relay as defined in TGCP. The BTX-4K is fully compliant with the TGCP specifications available online at http://www.cable-labs.com.

PacketCable CALEA Compliance

The BTX-4K complies with the Communications Assistance for Law Enforcement Act. The PacketCable Electronic Surveillance Specification describes how service providers must allow law enforcement agencies to intercept Call Content (media) and Call Signaling information.

The BTX-4K, as a Media Gateway, is designated as an Intercept Access Point for purposes of intercepting Call Content for calls originating on the PSTN and redirected back to the PSTN. For example, a Law Enforcement Agency must be able to intercept Call Content when a cable telephony subscriber uses Call Forwarding to redirect a call to an off-net number (that is, not associated with an MTA) in the PSTN.

PacketCable Security Compliance

PacketCable uses a set of algorithms to encrypt and authenticate both media and TGCP signaling.

IPsec

IPsec ESP security is utilized between the BTX-4K gateway and an MGC to ensure both the privacy and the message integrity of TGCP traffic.

AES, MMH, SHA-1

The BTX-4K supports AES encryption for both RTP and RTCP between the MTA and the BTX-4K to ensure voice call privacy. It also supports MMH authentication for RTP and SHA-1 authentication for RTCP.

Multiple MGC Connectivity

The BTX-4K allows up to 48 unique Media Gateway Controllers (MGCs) to control endpoints within a gateway. Each of the 6 DS3s, 2 STM-1s, or 2 OC-3s can be configured to be controlled by 8 unique MGCs. The MGCs are uniquely identified by IP address or domain name, and by UDP port address.

In the event of an MGC failure, a backup MGC can contact the BTX-4K with new routing information. Or, by enabling MGC Hunt in the BTX-4K, the TDM MGC table will be walked sequentially through the list of MGCs until an MGC provides an ACK to the gateway. The BTX-4K will then switch to this new MGC.

ISDN Backhaul

The ISDN backhaul over IUA/SCTP application allows layer 3 ISDN signaling transport across IP to a MGC or ASP. This mode is configured at the trunk level, on a per DS1 basis.

SNMPv3

SNMPv3 can be utilized to ensure integrity and privacy in all communications between the Nuera NetConductor and the BTX-4K gateway. Key management and key provisioning facilitate this capability.

DNS Lookup

MGCs can be identified by their domain name as well as by their network IP addresses. The BTX-4K can query a DNS server to determine an MGC's IP address based on the domain name.

BTX-4K supports up to two (that is, primary and secondary) DNS servers.

Force Connect

Force Connect allows static connections for RTP, RTCP and T.38 transport, as well as CAS and ISDN signalling transport, across IP without control from a softswitch. These connections occur at the trunk level, meaning that each DS1 can have a static connection to a different BTX-4K.

Voice Codecs

The BTX-4K supports G.711 µ-law, G.711 A-law and G.729AB voice codecs.

Echo Cancellation

Each voice channel in a BTX-4K gateway system meets or exceeds ITU G.168 recommendations for near-end echoes delayed by up to 64ms. The integrated echo canceller provides approximately 40dB of echo attenuation. The residual echo is further attenuated to imperceptible levels by a non-linear processing function. This is also referred to as NLP, center clipper, or residual echo suppressor. The NLP, as well as the echo canceller, can be disabled via configuration without interruption of voice processing.

Performance of an echo canceller is also a function of the echo return loss (ERL) provided by the 2-wire/4-wire hybrid. The echo canceller can operate with ERL values as low as 6dB.

Voice Activity Detection

The BTX-4K uses voice activity detection (VAD) to determine the difference between voice and background noise. When enabled, the VAD blocks the transmission of packets when voice is not present. When running PCMU or PCMA codecs, the VAD algorithm is Nuera proprietary based on neural net technology. When running the G.729A codec, the VAD algorithm is specified by G.729B.

Lost Packet Recovery / Packet Loss Concealment

The BTX-4K uses lost packet recovery (LPR), also known as packet loss concealment (PLC), to compensate for network disruptions that could result in late or lost packets at the receiver. When no packet is available for audio decoding, these adaptive algorithms are used to synthesize the audio signal based on prior observed statistics. When running PCMU or PCMA codecs, the LPR algorithm is Nuera proprietary based on neural net technology. When running the G.729A codec, the LPR algorithm is specified by G.729B.

Inband Signaling, Fax and Modem Support

The BTX-4K supports the following protocols:

- Inband Signaling: DTMF, MF, CAS, ISDN PRI
- Fax: V.21, V.27ter, V.29, V.17, V.34, T.38
- Modem: V.22, V.32, V.34, V.9x, V.18(TTY)

Differentiated Services (Diffserv)

Diffserv can be used to prioritize voice traffic over data traffic in an IP network. Diffserv takes the IP Type of Service (TOS) field, renames it the DS byte, and uses it to carry information about IP packet service requirements. Diffserv relies on traffic conditioners sitting at the edge of the IP network to indicate each packet's requirements (i.e. priority).

BTX-4K allows administrators to configure the DS byte for signaling (TGCP), media (RTP/RTCP) and configuration (SNMP). This enables network administrators to manage quality of service through the Managed IP Network.

TFTP Access List

The BTX-4K supports an access list of up to three (3) clients (NetConductor and two additional, user-specified clients) allowed to perform TFTP downloads to the gateway.

Syslog

The BTX-4K can export debug logs to a Syslog server. The BTX-4K utilizes the Syslog standard for message format and provides an expanded debug configuration for multiple subsystems via SNMP. Standard off-the-shelf monitoring tools can be used to collect the Syslog messages to enable troubleshooting.

Physical Connections

The following physical interfaces exist on the BTX-4K gateway:

- The PSTN telephony interfaces:
  - DS3
  - OC-3 (SONET)
  - STM-1 (SDH)
- BITS clock inputs. This T1/E1 interface provides the clock to the system.
- The GigE interface, also called the Media Interface. This transports packetized media traffic to and from the gateway and can be configured to support TGCP signaling traffic.
- The 100 BaseT interface, also called the Control Interface. This carries the SNMP management traffic on a separate physical network from the voice. TGCP signal-

ing is configurable on either the Media Interface or Control Interface.

- Craft interface. This serial interface is used for initial configuration (gateway IP address, subnet mask, default router) of the gateway.
- Alarm interface. This interface connects the gateway to external alarm collectors.

Typical Network Application Configuration

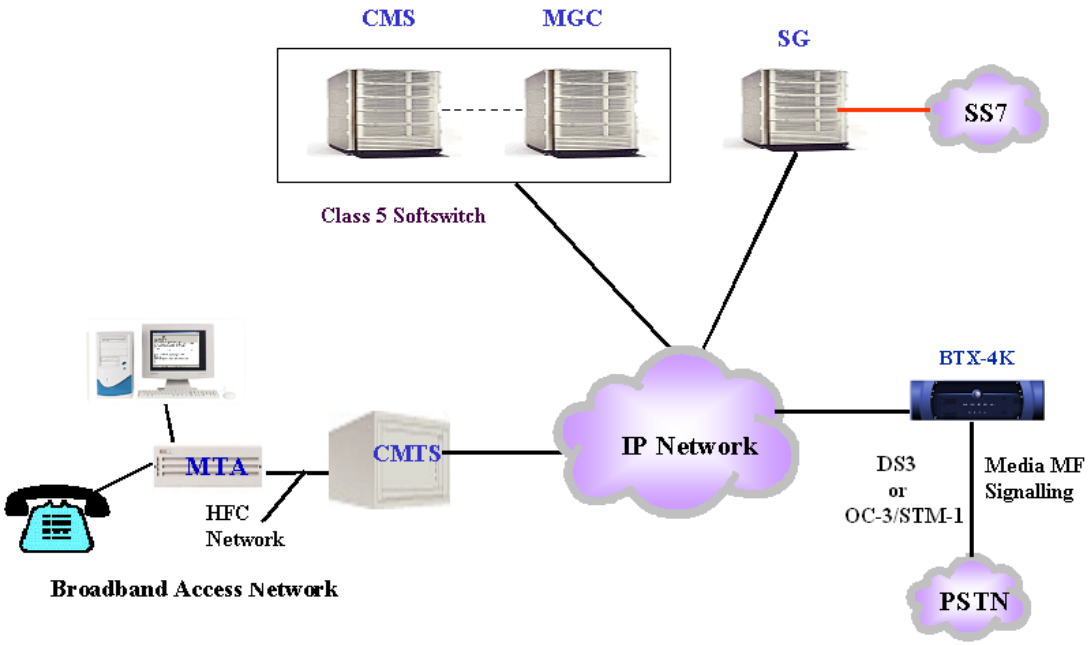


Figure 1. BTX-4K PacketCable Network Application

Figure 1 shows a graphical representation of a network application for the BTX-4K gateway. The gateway is designed to provide a bridge between packet-switched telephony networks and existing public telephone networks, by terminating and controlling physical circuits in the form of bearer channels from the PSTN. This section also provides a basic understanding of supported network protocols, functional features, and how the BTX-4K conforms to PacketCable standards.

BTX-4K in a PacketCable Network

PacketCable™ is a project conducted by Cable Television Laboratories, Inc. (CableLabs®) and its member companies. PacketCable defines interface specifications used to develop interoperable equipment capable of providing packet-based voice, video, and other high-speed multimedia services over hybrid fiber coax (HFC) cable systems using the DOCSIS 1.1 standard. PacketCable defines a network superstructure that overlays the two-way data-ready broadband cable DOCSIS 1.1 access network.

The BTX-4K fulfills the role of a Media Gateway between the packet network and the PSTN. It performs the following functions:

- Terminates and controls physical circuits in the form of bearer channels from the PSTN.
- Processes channel associated signaling (CAS), if applicable.
- Detects events on endpoints and connections as requested by a Media Gateway Controller.
- Generates signals on endpoints and connections (for example, continuity tests, ring tone, and so on), as instructed by the Gateway Controller.
- Creates, modifies, and deletes connections to and from other endpoints as instructed by the Media Gateway Controller.
- Controls and assigns internal media processing resources specific connections upon receipt of a request from the Media Gateway Controller.
- Performs all media processing between the PSTN and the network.
- Ensures that any entity communicating with the Media Gateway adheres to the security requirements.
- Stores and reports connection and channel statistics.

CableLabs Certification

The CableLabs Certification Process has been developed to provide cable operators with confidence that the certified equipment is built to the project specifications and, therefore, interoperates with other CableLabs certified products made by other vendors.

Certification is achieved by successfully completing an Acceptance Test Plan (ATP). ATPs consist of Compatibility Test Plans (CTPs). CTPs are executed and evaluated in Certification Waves (CWs) held quarterly.

The BTX-4K supports the functionality required to comply with all aspects of the TGCP, Security, CALEA and Codec CTPs. The BTX-4K also provides value-added functionality needed by leading-edge Cable MSOs.

BTX-4K in a Force Connect Application

The Force Connect application, as shown in Figure 2, allows static connections for RTP transport as well as CAS and ISDN signaling transport across IP without control from a softswitch. The granularity of these connections is at the trunk level, meaning each DS1 can have a static connection to a different BTX-4K. You can select

from two modes: force connect for bearer only channels (i.e. for ISUP CIC trunks or CAS trunks), or force connect PRI with signaling and bearer channels (i.e. ISDN PRI trunks).

Figure 2. BTX-4K Force Connect NetworkApplication

Nuera NetConductor

The Nuera NetConductor is a web-based client/server Element Management System (EMS) that enables operators to configure, monitor, and control all the ORCA gateways in a network. The NetConductor lets you easily recognize fault conditions, then isolate a problem to a particular subsystem or network component. You can use a single tool for monitoring network events and alarms.

The NetConductor also collects data at user-specified intervals to compile statistics that help manage throughput and response time. In addition, you can define alerts to detect degrading network performance.

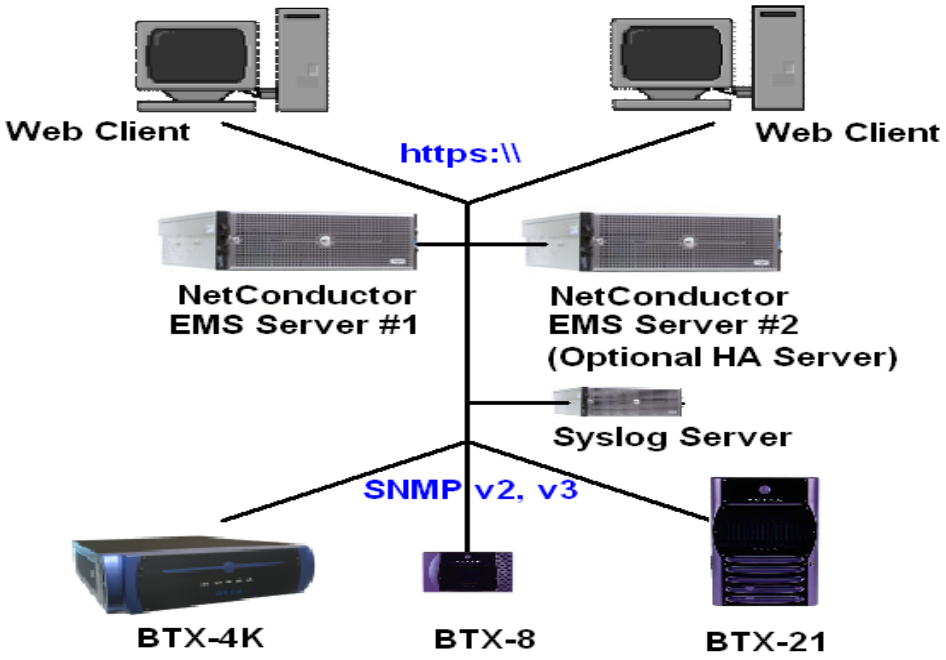


Figure 3. EMS Network Layout

NetConductor (EMS) Network Layout

As shown in the network layout in Figure 3, you can manage your gateways with a server and web client combination. Using a standard web browser, you can access the Nuera NetConductor EMS to configure your gateways. Client-side web browsers use a secure web interface (https) to communicate with EMS, which then communicates with the BTX-4K using the SNMP protocol.

SNMPv3

SNMPv3 addresses issues related to the large-scale deployment of SNMP, accounting, and fault management. Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

SNMPv3 performs the following functions:

- Verifies that each received SNMP message has not been modified during its transmission through the network.
- Verifies the identity of the user on whose behalf a received message claims to have been generated.

- Detects received messages that contain management information, whose time of generation was not recent.
- Ensures that the contents of each received message are protected from disclosure.

2

GETTING STARTED

This chapter covers the initial configuration of the BTX-4K, including procedures for verifying the physical connections and setting the network configuration information.

This chapter also provides an introduction to the basic functionality of the NetConductor web client. For a more complete discussion of the NetConductor software, see the *NetConductor User's Guide*. Remaining chapters in this manual will cover configuration and monitoring functions specific to the BTX-4K using NetConductor.

Craft Port

The craft port plays a small but crucial part in bringing a BTX-4K gateway online. This DB9 (male) connector that provides a serial interface is located on the BCM card on the back of the gateway, and is labeled the "Craft" port. It is used to connect a computer directly into the gateway to assign basic configuration information.

After connecting a computer to the port, you can use a terminal emulation program to access the gateway.

To access the gateway:

1. Connect the serial cable from the computer to the craft port on the active card.
2. Open the **HyperTerminal** (or other terminal software emulation) dialog.
3. Use the settings shown in Figure 4 to correctly configure the emulation program:

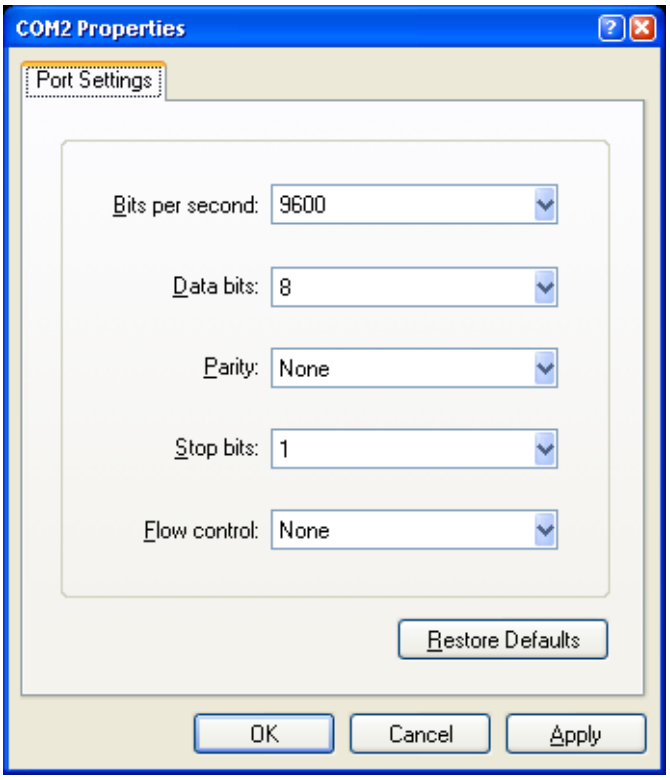


Figure 4. HyperTerminal Settings

4. Press **Enter** if you don't see the **Password** prompt.
5. At the **Password** prompt, enter a password. The default password is **nuera**.
6. Press **Enter**.

At the User prompt type **help** or **?** to see the list of available commands. These craft port commands serve to configure the gateway IP addresses. For a more detailed description of these commands, see the *ORCA-4K Hardware Manual*.

Take special care with your password as there is no way to recover a lost password.

IP Address Configuration

Before you can configure the gateway using NetConductor, you must set up the IP addresses via the Craft interface port. Verify that the IP addresses assigned to your gateway are not used anywhere else in your network.

Use the *Ethernet show* command at the craft port to view configured IP addresses. This command shows the fixed and floating Ethernet settings for the control and media ports. You must set six IP addresses for the gateway:

- One floating IP address for management (control) messages.
- Two background IP addresses for Voice Processing Modules (VPMs).
- One floating IP address for media.
- Two background Media IP addresses for VPMs.

Media and management can be on different subnets but the background IP for media must be on the same subnet as the floating IP for media. This also applies for the control port.

After you have set the gateway IP addresses, you must configure the Default Gateway IP address and subnet mask using Craft port controls to facilitate a network connection. Next you must configure the Base Media UDP port and the Call Control Signaling Interface. Once the BTX-4K gateway is connected to the IP network, you can perform the remaining configuration tasks via SNMP using a Nuera NetConductor server or the NetConductor Local Interface.

For a list of craft port commands or instructions for configuring the gateway through the craft port, see the *ORCA-4K Hardware Manual*.

Physical Connections

Nuera recommends that you make the following gateway connections before creating your Network Elements:

- Power
- Ethernet (100BaseT and 1000BaseSX aka GigE)
- DS3 or optical (OC-3/STM-1)
- BITS Clock
- Craft Interface
- Alarm Port (optional)

For more information on the physical connections on your gateway, see the *ORCA-4K Hardware Manual*.

Accessing NetConductor

Enter the IP address, including the port number, of the NetConductor server into the address bar of your browser. For example, http://172.16.103.99:5960. (See your network administrator for the IP address and corresponding port number of your NetConductor server. The default port number is 5960.)

Upon connection with the NetConductor server, your browser will display a splash screen with the Nuera logo and a Login button. Click this button, then enter your username and password (and server name, if applicable) in the window that displays, as shown in Figure 5.

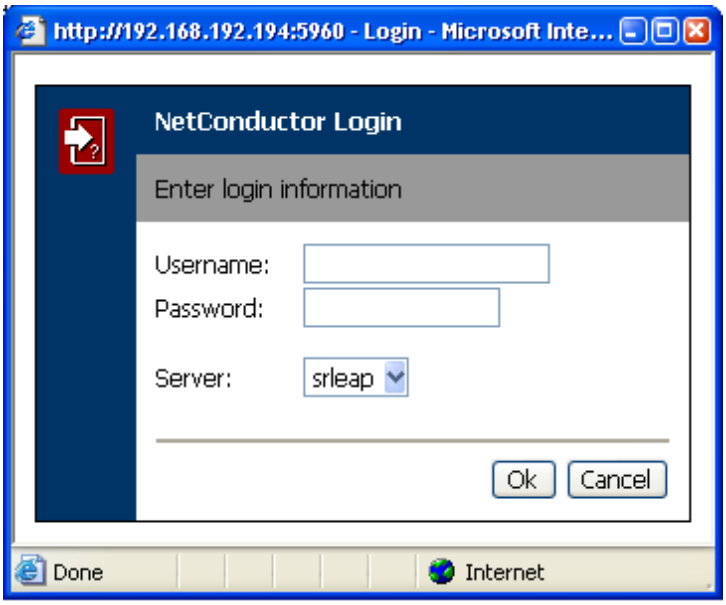


Figure 5. NetConductor Login window

The User Interface

The main screen of the NetConductor web client is divided into four separate frames, or panes. As shown in Figure 6, the NetConductor interface includes a Links pane, Navigation pane, Information pane, and Alarm pane.

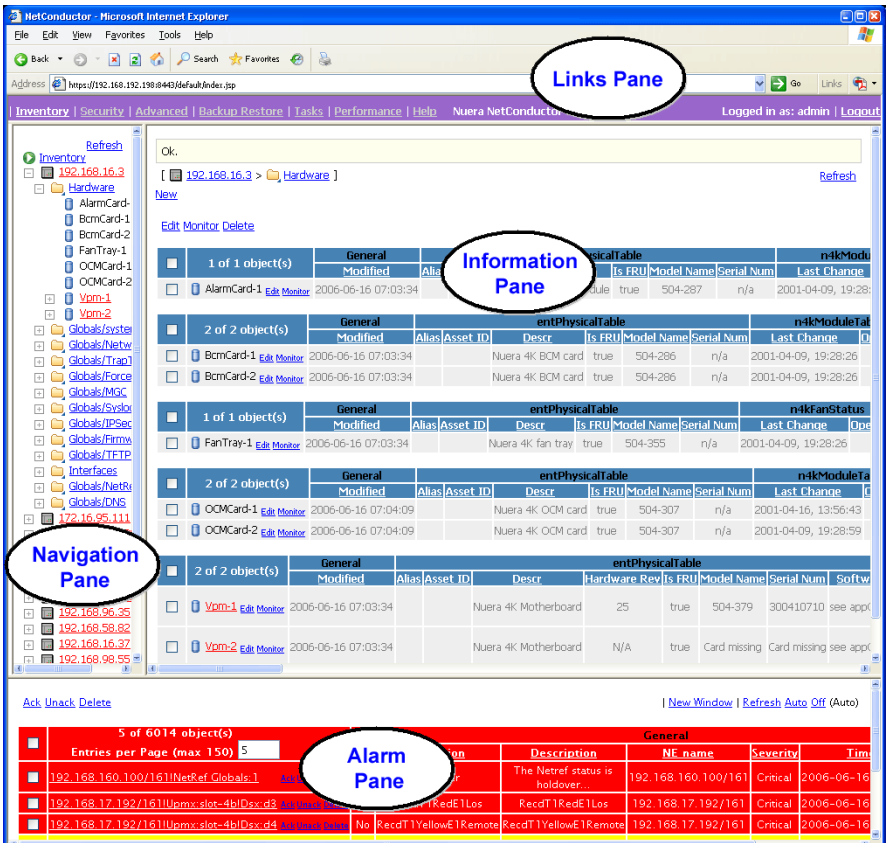


Figure 6. The NetConductor Interface

Links Pane

The links at the top of the page allow you to access a variety of NetConductor functionality. From these links, you can view and configure network elements, access user profiles or server core functions, as well as logout. Specifically, these links are:

- **Inventory** - Displays a list of all the Network Elements (NEs)
- **Security** - Access user profile management
- **Advanced** - Access server core functions intended for the system administrator
- **Backup Restore** - Backup and restore the configuration of a selected Network Element
- **Tasks** - Review a variety of summary information generated for each Network Element and upgrade firmware, capacity and vocoder capability.
- **Performance** - Create and manage performance schedules for a selection of network entities.

Navigation Pane

The Navigation pane is the starting point for configuring and managing your Network Elements. Use the hierarchy in this pane, as shown in Figure 7, to easily locate and select specific network components.

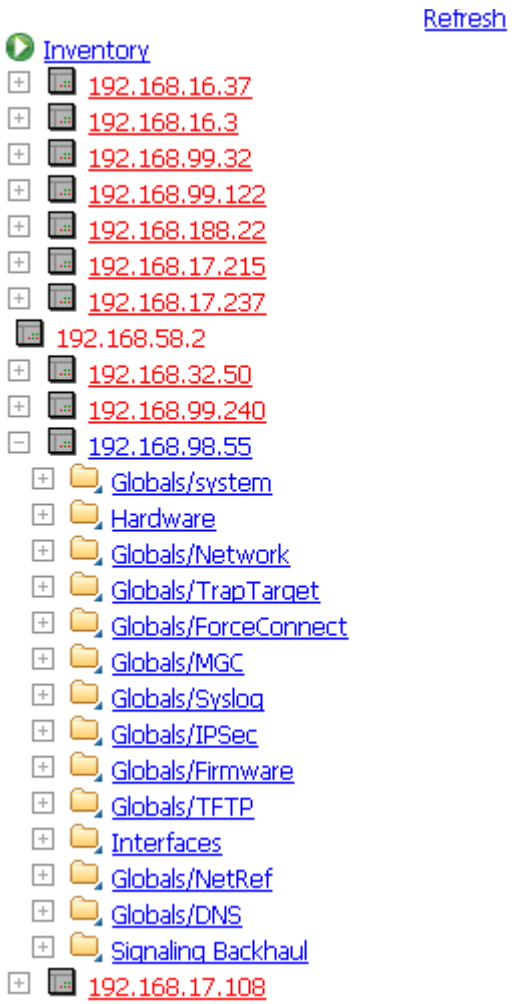


Figure 7. NE Hierarchy in the NetConductor Navigation pane

This figure shows the hierarchy of configurable components for a specific Network Element (NE) called *192.168.98.55*. From this view, you can click on any of these components to display the corresponding settings in the Information pane.

Information Pane

The Information pane displays statistical and configuration data specific to the item you selected in the Navigation pane. For instance, by selecting **Hardware > VPM-1**

in the Navigation pane, you can display a list of corresponding VPMs in the Information pane, as shown in Figure 8.

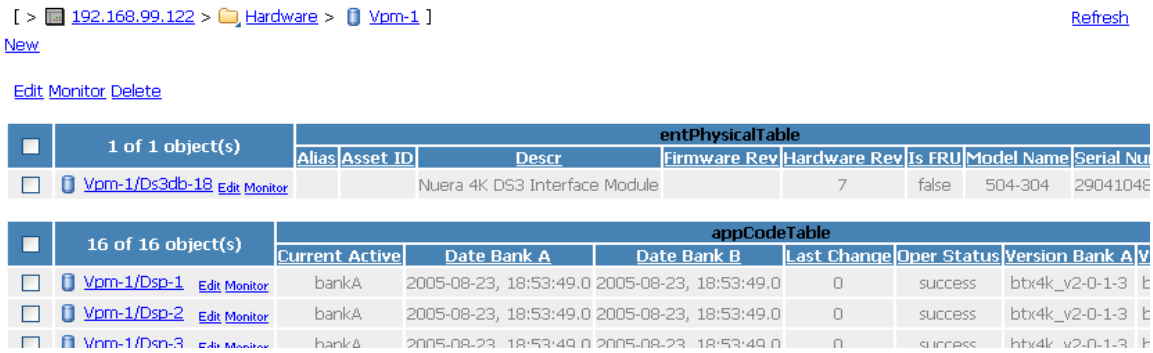


Figure 8. Information pane

The Information pane shown in Figure 8 displays information about the two installed VPMs. Using the links above the list of components, you can **edit**, **monitor**, and **delete** components as necessary. Notice that you can select and edit multiple components simultaneously.

After selecting the **edit** or **monitor** links or the component link directly, the Information screen will change to show the specific settings for the selected component. See Figure 9 for an example of this screen.

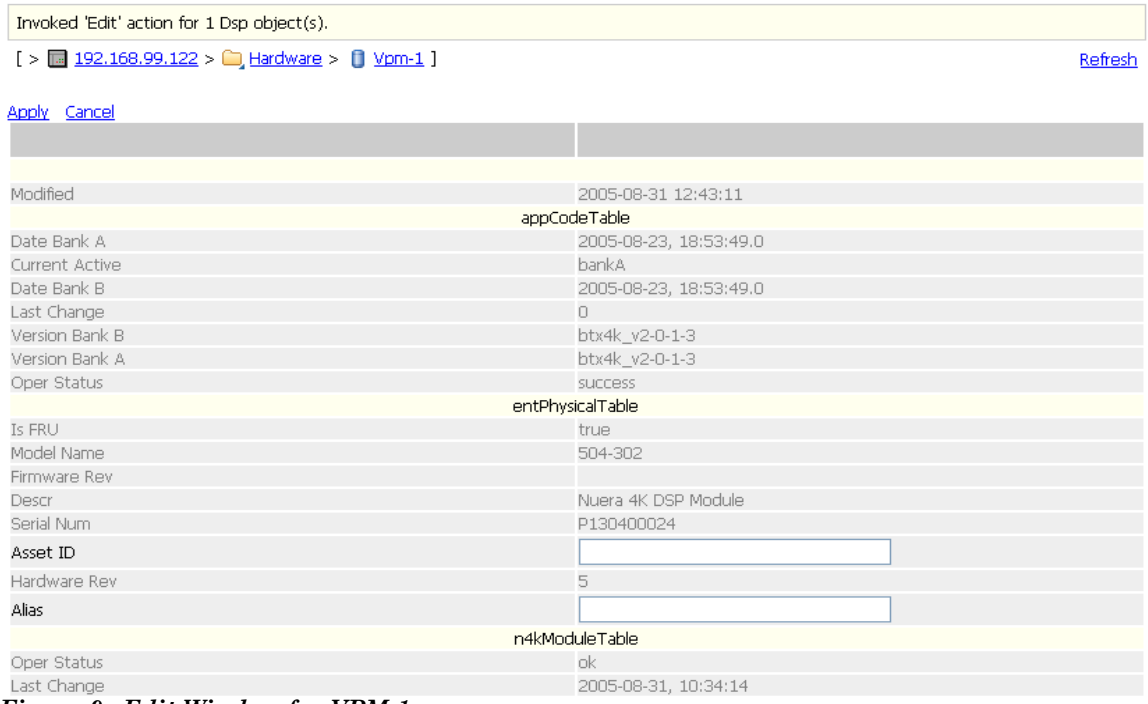


Figure 9. Edit Window for VPM-1

From the monitor window, you can manually **refresh** the server to retrieve the latest status and statistical data, or use the tabs at the top of the window to automatically refresh every 10 or 60 seconds. This can be useful when monitoring or troubleshooting a specific network component.

Alarm Pane

The Alarm pane, as shown in Figure 10, displays a list of alarms sent from the monitored NE. Each alarm is timestamped upon receipt by the server, with the most recent alarms at the top of the list. The background color of the alarm displays the severity of the alarm:

Alarm Color	Severity
Red	Critical
Orange	Major
Yellow	Minor
White	Informational
Light Purple	Disconnected

The first two alarms shown in Figure 10 are Critical alarms and the last is a Major alarm.

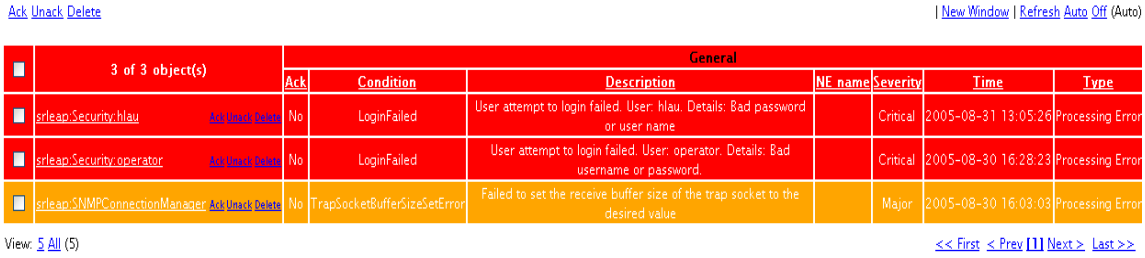


Figure 10. Alarm pane

You can sort any of the columns in the alarm pane by ascending or descending order. The green arrow in the heading of the "Time" column shows that column sorted in descending order, with the most recent alarm at the top. From the upper right hand corner of the pane, you can refresh the alarm pane by clicking **Refresh** or automatically refresh every ten seconds by selecting **Auto**.

Managing Alarms

NetConductor recognizes and displays two types of alarms: latched and non-latched alarms. Typically a latched alarm reports an underlying problem that requires resolution. Non-latched alarms are informational alarms, often announcing instantaneous event notification, and do not require action or resolution.

Example - Latched Alarm

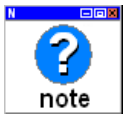
An example of a latched alarm would be when the DS3 interface displays an alarm because the cable is unplugged. This alarm could be cleared by plugging in the cable.

Example - Non-Latched Alarm

An example of a non-latched alarm is the notification "**User attempt to login failed. User: EMSuser. Details: Bad password or user name.**"

The type of alarm often determines your response. After viewing a non-latched alarm like a failed login, you may simply want to delete the alarm. You can do this by selecting the alarm, then clicking **Delete** in the upper left of the pane. For a latched alarm that requires a definitive resolution, e.g. plugging in the cable on your DS3 interface, you can choose to acknowledge (**Ack**) the alarm before going to the gateway to fix the problem manually. By Acking the alarm in this way, you signify to other network operators that you have acknowledged the alarm and are attempting to resolve the

problem. An alarm may be unacknowledged by selecting **UnAck**. This feature can save you and your team from duplicating complicated troubleshooting efforts.



You can also delete a latched alarm from NetConductor, but the alarm will reappear upon repolling the Network Element if you have not resolved the underlying problem.

3

CONFIGURING RESOURCES

This chapter describes how to configure your gateway through the graphical user interface (GUI) of the NetConductor EMS.

Prerequisites

The instructions detailed in this chapter describe how to bring up a gateway and start processing calls. These steps assume the following:

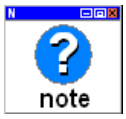
- The correct version of NetConductor is installed on the server.
- You have a Syslog Collector application installed on a server separate from the NetConductor server.
- The physical Ethernet connections are present.
- The gateway is correctly configured from the Craft port command line (documented in the *ORCA-4K Hardware Manual*), including the IP addresses, masks, and default routers.
- Dual BITS sources are plugged into the BITS T1/E1 ports. If BITS sources are unavailable, a specific TDM interface can be used. For more information, see "Configuring NetRef" on page 39.
- The external TDM connections are up (i.e. ready for the gateway to be configured).

Initial Configuration

Use the hierarchy of network components in the NetConductor navigation pane to access a list of gateways and corresponding configuration folders. The remaining sections in this chapter will detail the following steps required to bring up a gateway and start processing calls:

To configure your gateway:

1. Add a Network Element.
2. Configure the BITS Clock.
3. Configure NETREF.
4. Configure DNS.
5. Configure IPsec.
6. Configure Media Gateway Controllers (MGCs) for TGCP applications.
7. Configure Remote Gateways for Force Connect applications.
8. Configure the TDM Interface.
9. Configure DS1 and Media Parameters.
10. Configure the Network Globals.
11. Configure the TrapTarget.
12. Configure the TFTP Client.
13. Configure System Globals.
14. Configure Hardware Settings.
15. Configure IUA.



The configuration parameters detailed in this chapter are also available in the Nuera NetConductor Online Help System. Select the Help link in any NetConductor Information pane, to launch the Help System in a new browser window.

Adding a Network Element

A Network Element (NE) is a software representation of a gateway that will be monitored and controlled by the NetConductor EMS. Before you can begin monitoring your gateway, you must first create an NE within NetConductor.

SNMPv3 is the default protocol, but the system will also accept SNMPv2 if it is configured via the craft port. At the gateway's craft port, you can set the gateway to accept SNMPv2 with the following command:

snmpcfg procv2 on

To create a new Network Element (NE):

1. Select **Inventory** from the list of links at the top of the main window to display a list of Network Elements in the Information pane.
2. From the Information pane, click **New** to display the Create New NE window, as shown in Figure 11.

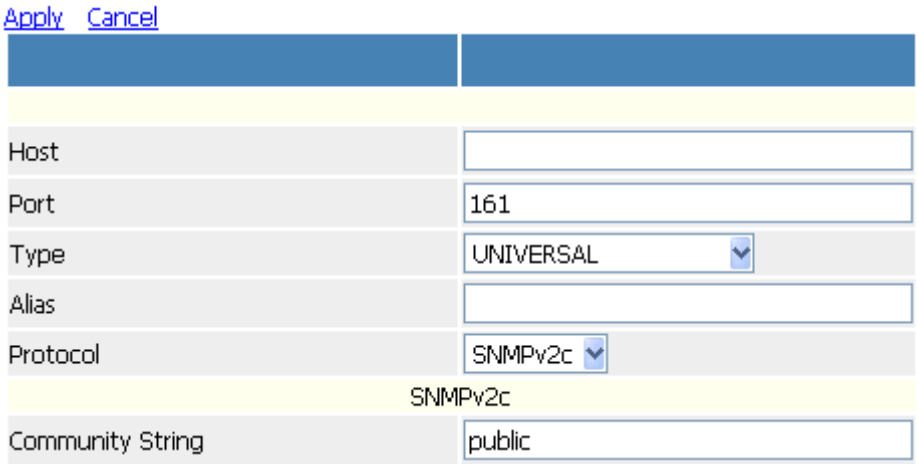
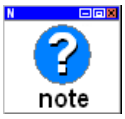


Figure 11. Create New NE, Step 1

3. The **Host** parameter allows you to define the network location of the NE. Configure the **Host** parameter with the IP hostname or valid IP address for the NE.
4. Configure the **Port** field to **161**.
5. Choose the **Type** from the drop-down box. The **Type** is dependent on the type of NE and desired software version.
6. The **Alias** parameter allows you to give the new NE a name. The **Alias** field has no networking properties.
7. The **Protocol** drop-down box allows you to match the SNMP version being transmitted by the NE. Available selections are **SNMPv2** and **SNMPv3**.
   - If you select **SNMPv2** you will be prompted to enter the community string.
   - If you select **SNMPv3** you will be prompted to enter the **User Name** and **Passphrase** of the NE.

The SNMPv2 community string must match what is configured via the craft port. For more information about configuring the gateway through the craft port, see the *ORCA 4K Hardware Manual*.

8. Click **Apply** to finish adding the NE.



NetConductor will take a few seconds to verify the settings and synchronize with the gateway. The newly added gateway will then appear in the Navigation pane hierarchy. Once you add a new network element, the server will start polling it. In the Net-Conductor information pane, the poll state of your new network element should read "NE_POLL_IN_PROGRESS". When this status returns to "IDLE", the server has gathered all the information for the new Network Element.

Configuring the BITS Clock

You can set two BITS clocks to provide redundant timing for the gateway. When using DS3 or OC-3 configured Optical VPMs, only the T1 BITS clock interface is supported. When using STM-1 configured Optical VPMs, only the E1 BITS clock interface is supported.

To set the BITS clock source:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces.**
2. Select **BITS** to display a list of BITS clock sources in the Information pane, as shown in Figure 12.

Edit Monitor Delete

	2 of 2 object(s)	ifTable						General
		Admin Status	Descr	Last Change	Oper Status	Speed	Type	Modified
☐	Bits-1 Edit Monitor	up	bits 1	2005-09-06, 11:45:32	up	0	ds1	2005-09-06 12:14:32
☐	Bits-2 Edit Monitor	up	bits 2	2005-09-06, 11:45:32	up	0	ds1	2005-09-06 12:14:32

Figure 12. BITS Information pane

3. Select **Edit** to the right of the BITS Clock to display the corresponding parameters in the Information pane, as shown in Figure 13.

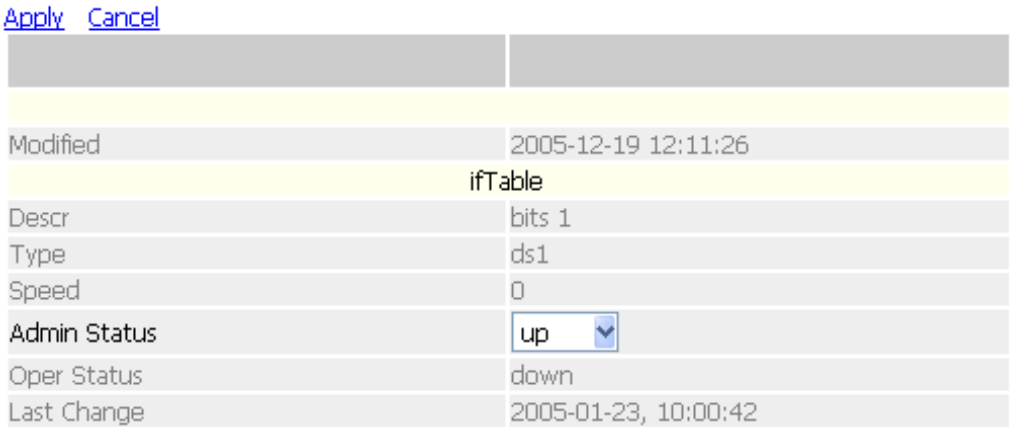


Figure 13. BITS General Statistics

4. Configure **Admin Status** to **up**. This is the desired state of the physical interface.
5. Select **Apply**.
6. Repeat these steps for **BITS-2**, the other BITS clock source.

The BITS clock Oper Status may remain down until it has been assigned as a NetRef. See "Configuring NetRef" on page 39.

Configuring NetRef

The Network Reference Clock (NetRef) is the clock source used to synchronize the TDM signals into and out of the system. In most cases, the BITS clock is used as the network reference clock, but you may also select a DS1, OC-3, or STM-1 interface for this purpose.

It is important to configure both the primary and secondary NetRefs to avoid clock slips.

Mixing BITS with a DS1, OC-3, or STM-1 interface for the network reference clock is not supported in this release. In setting your primary and secondary clocks, you must set both clocks to either BITS or TDM interfaces.

To configure the NetRef:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/NetRef** to display the NetRef Information pane as shown in Figure 14.

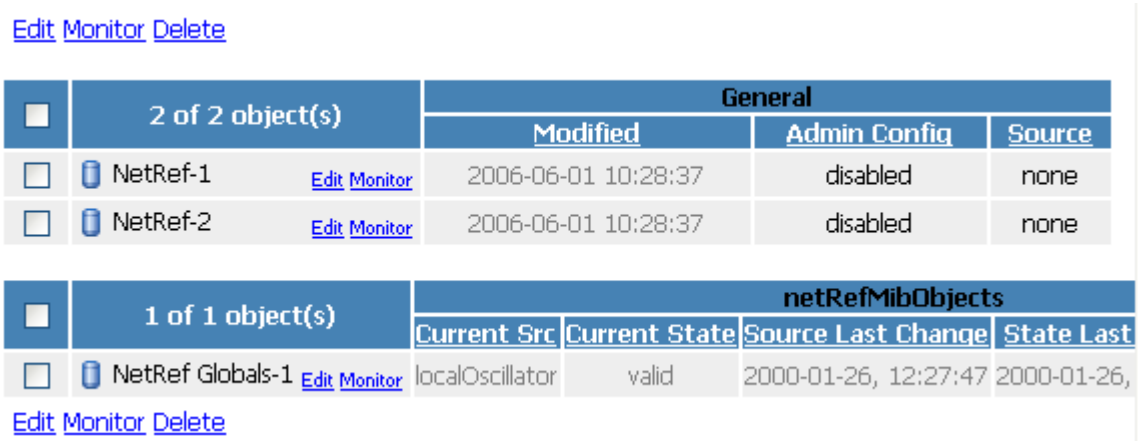


Figure 14. NETREF Information pane

2. Click **Edit** to the right of the NETREF to configure the corresponding parameters in the Information pane, as shown in Figure 15.

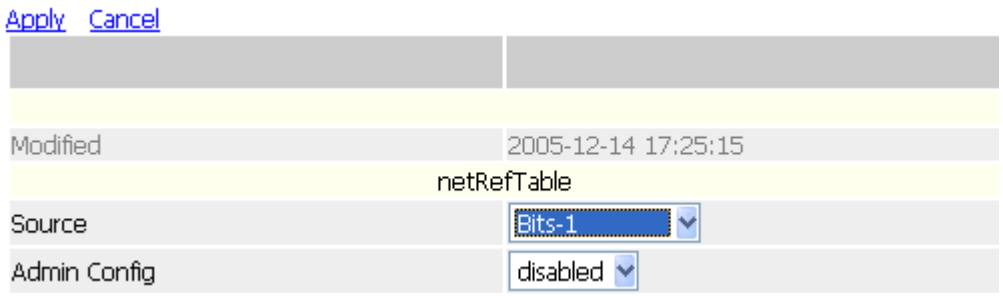
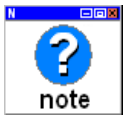


Figure 15. NETREF General Statistics

3. Configure the **Source**. This setting indicates the physical interface from which to clock NETREF. If you select none, the local oscillator will be used.
   - If your BTX-4K has a **metallic DS3** interface, you have 171 different choices for the clock source: none, BITS-1, BITS-2, or any of the 168 channelized DS1 interfaces, e.g., DS3-6/DS1-28.
   - With an **optical OC-3** interface, you have 7 choices for the clock source: **none**, **Bits-1**, **Bits-2**, **OC3-1/WORKING-1**, **OC3-1/PROTECT-1**, **OC3-2/WORKING-1**, and **OC3-2/PROTECT -1**.
   - With an **optical STM-1** interface, you have 7 choices for the clock source: **none**, **BITS-1**, **BITS-2**, **STM1-1/WORKING-1**, **STM1-1/PROTECT-1**,

STM1-2/WORKING-1, and **STM1-2/PROTECT-1**.



When setting the NETREF Source for any interface, verify that the interface is online.

4. Set **Admin Config** to **enabled**. When disabled, the clock source is not a candidate for source of network timing.
5. Select **Apply**.
6. Repeat these steps for the second NETREF.

Configuring DNS

From the **Globals/DNS** folder, you can enter the address of your DNS server and enable or disable DNS usage on the gateway.

To configure the DNS:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/DNS** to display the DNS Server Information pane as shown in Figure 16.

Edit Monitor Delete

1 of 1 object(s)	dnsUserMibObjects	General
	Clear Cache Op	Modified
DNS Globals-1 Edit Monitor	none	2006-06-01 10:28:38

3 of 3 object(s)	dnsUserResolverTable			
	Address	Fqdn	Status	Time To Live
DNS Resolver-1 Edit Monitor	192.168.24.9	192.168.24.9	not-applicable	2147483
DNS Resolver-2 Edit Monitor	192.168.25.13	192.168.25.13	not-applicable	2147483
DNS Resolver-3 Edit Monitor	192.168.24.41	192.168.24.41	not-applicable	2147483

2 of 2 object(s)	dnsUserServerTable				
	Address	Admin Config	Index	Oper Status	Oper Stat
DNS Server-1 Edit Monitor	0.0.0.0	disabled	primary	down	2000-0
DNS Server-2 Edit Monitor	0.0.0.0	disabled	secondary	down	2000-0

Edit Monitor Delete

Figure 16. DNS Server Information pane

2. To configure the primary server, click **Edit** to the right of the **DNS Server-1** link to display the corresponding parameters in the Information pane, as shown in Figure 17.

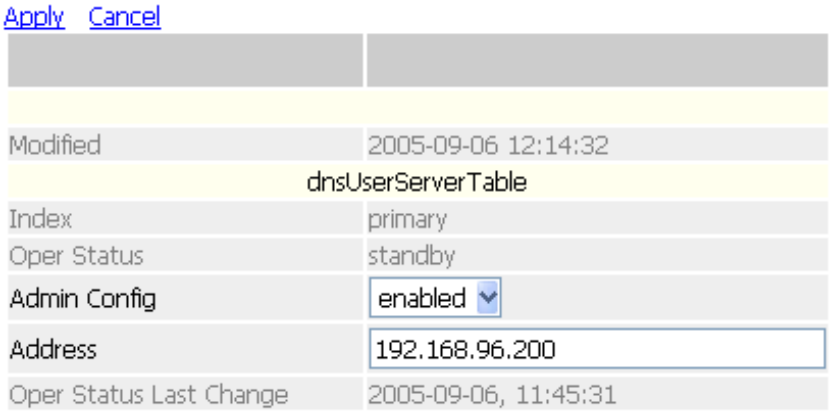


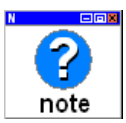
Figure 17. DNS Server General Statistics

3. Configure the **Address** with the IP address of the DNS server.
4. Set the **Admin Config** to **enabled**.
5. Select **Apply**.

   To enter a secondary DNS, repeat these steps using DNS Server-2.

Configuring IPsec

There are 51 configurable IPsec templates. Each template is referenced by an index number from 1 to 51. There is a one to one correspondence between the IPsec template and an MGC template. You should configure each template with the IPsec configuration parameters matching your MGCs. There is no requirement that the Index of the IPsec template match that of the Index to the MGC Template. If you plan to use TFTP over IPSEC, you should leave one IPSEC template blank for use by NetConductor. See "Configuring Media Gateway Controllers for TGCP Applications" on page 44 for more information on how to link these templates.



IPsec is not used for Force Connect applications and does not need to be configured.

To configure an IPsec template:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/IPsec** to display

the IPSec Information pane as shown in Figure 18.

Edit Monitor Delete
51 of 51 object(s)
Modified
IKE Diffie
IPSec Template-1 Edit Monitor 2005-09-01 12:01:54
IPSec Template-2 Edit Monitor 2005-09-01 12:01:54
IPSec Template-3 Edit Monitor 2005-09-01 12:01:54
IPSec Template-4 Edit Monitor 2005-09-01 12:01:54
IPSec Template-5 Edit Monitor 2005-09-01 12:01:54

Figure 18. IPsec Information pane

2. Click **Edit** to right of the template to display the corresponding parameters in the Information pane, as shown in Figure 19.

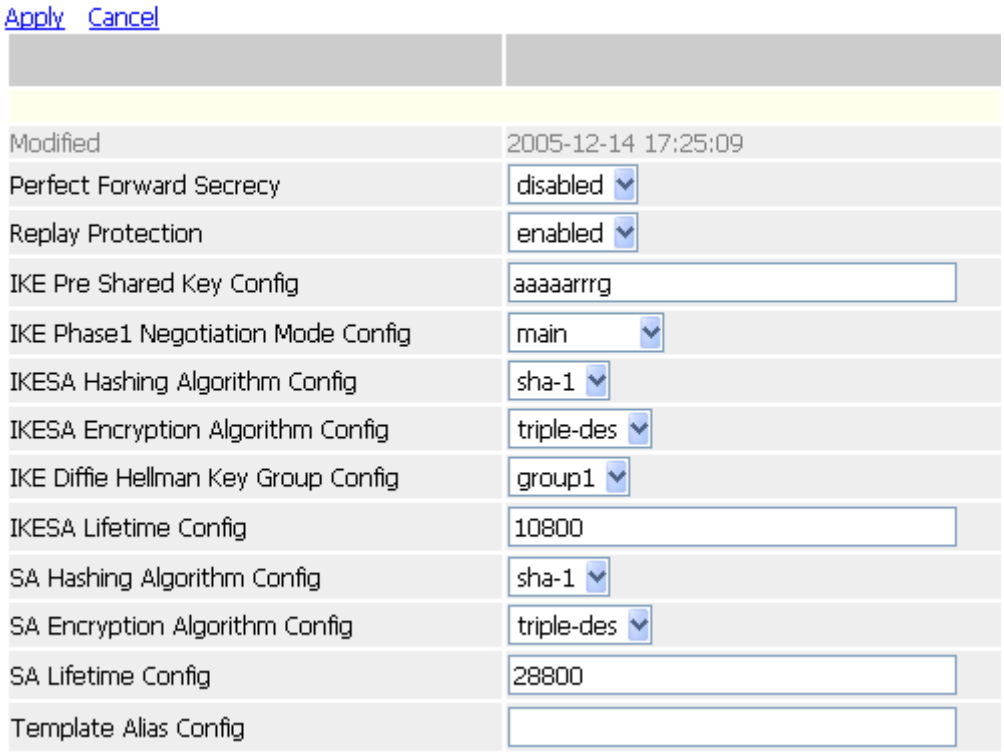

Apply Cancel
Modified 2005-12-14 17:25:09
Perfect Forward Secrecy disabled
Replay Protection enabled
IKE Pre Shared Key Config aaaaarrrg
IKE Phase1 Negotiation Mode Config main
IKESA Hashing Algorithm Config sha-1
IKESA Encryption Algorithm Config triple-des
IKE Diffie Hellman Key Group Config group1
IKESA Lifetime Config 10800
SA Hashing Algorithm Config sha-1
SA Encryption Algorithm Config triple-des
SA Lifetime Config 28800
Template Alias Config

Figure 19. IPsec General Statistics

3. Select the **IKESA Hashing Algorithm Config**.
4. Select the **IKESA Encryption Algorithm Config**.

5. Enter the **IKE Pre Shared Key Config** that matches the MGCs preshared key. This key is entered in ascii text and will be displayed.
6. Select the **IKE Diffie Hellman Key Group Config**.
7. Select the **SA Encryption Algorithm Config**.
8. Enter the **SA Lifetime Config**. This is the lifetime of the IPsec SA tunnel, in seconds.
9. Configure the **Replay Protection**. This service protects against replay of self-contained packets that already have a cryptographical integrity mechanism in place.
10. Configure **Perfect Forwarding Secrecy**. The condition in which the compromise of a key after a given session does not cause the compromise of any earlier session.

Perfect Forwarding Secrecy is not used in this release.

11. Select the **IKE Phase 1 Negotiation Mode Config**. Main mode = more secure; aggressive mode = less secure. Aggressive mode reveals the identity of the participants.
12. Enter the **IKESA Lifetime Config**. This value is the lifetime of the IKE SA tunnel, in seconds.
13. Select the **SA Hashing Algorithm Config**.
14. The **Template Alias Config** is a user defined name for the selected IPsec template.
15. When you have completed your configuration, select **OK**.
16. Repeat these steps for each IPsec Template you want to configure.

Configuring Media Gateway Controllers for TGCP Applications

The Media Gateway Controller (MGC) is the component of the Class 5 Softswitch Controller that controls the BTX-4K. The BTX-4K allows up to 48 unique MGCs to control endpoints within a gateway. Each of the six DS3s can be configured to be controlled by eight unique MGCs. Alternately, each of the OC-3 or STM-1 Working/Protect pairs (i.e. APS groups) can be configured to be controlled by 8 unique MGCs for a total of 16 unique MGCs for the optical application. The MGCs are uniquely identified by IP address or domain name, and by UDP port address.

In the event of an MGC failure, a backup MGC can contact the BTX-4K with new routing information. By enabling MGC Hunt, the interface MGC table will be walked sequentially through the list of MGCs until an MGC provides an ACK to the gateway. The BTX-4K will then switch to this new MGC.

Using DNS, the gateway will search the list of resolved IPs for the MGCs domain name should the initial (original) IP fail to respond to the gateway. The BTX-4K supports up to 10 resolved IP addresses per domain name.

MGC Configurables are not applicable to Force Connect applications.

To configure the Media Gateway Controller Templates:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/MGC** to display the MGC Template Information pane shown in Figure 20.

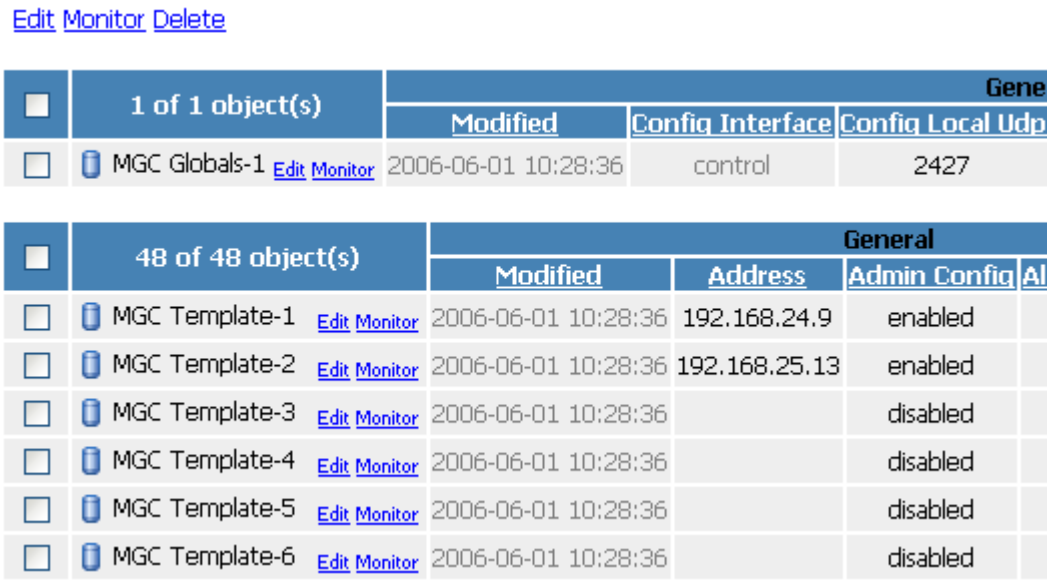


Figure 20. MGC Template Information pane

2. Click **Edit** to the right of the MGC template to display the corresponding parameters in the Information pane, as shown in Figure 21.

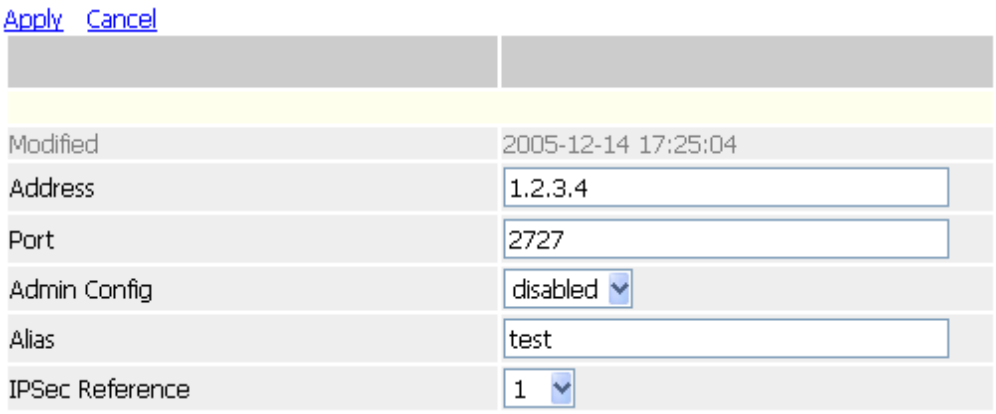
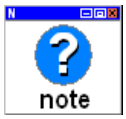


Figure 21. MGC Template General Statistics

3. Configure **Address**. This is the IP address or FQDN of the MGC. This value can be either a symbolic DNS name or in dot-quad notation.
4. Configure **Port**. This value is the number for the UDP port the gateway sends on; that is, that the MGC receives on.



Each MGC template should have a unique IP:UDP pair. If there are 2 MGC templates with the same IP:UDP pair then the first template in the list will dictate the security policy for that IP:UDP pair for the system.

5. Configure **Alias**. This is a user-defined name for this MGC server. It does not need to correspond to address name.
6. Configure **IPSec Reference**. This is the alias (and number) of the IPsec Template to be used when communicating with the MGC. The default value is "none", i.e. no security. You must change this to enable IP Security with the MGC.
7. Configure **Admin Config** to **enabled**.
8. Select **Apply**.
9. Repeat these steps for each MGC you want to configure.

When you have completed these steps, the FQDNs will resolve and you can view them by selecting **Inventory >** [NE] **> Globals/DNS** > **DNS Resolver**.

To configure MGC Globals:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/MGC** to display

the Information pane as shown in Figure 22.

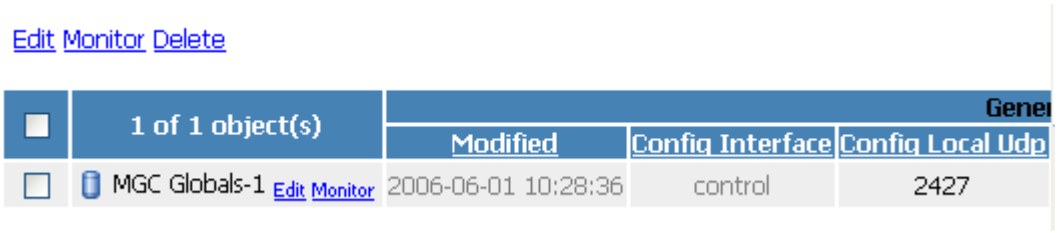


Figure 22. MGC Globals Information pane

2. Select **MGC Globals-1** and click **Edit** to display the corresponding parameters in the Information pane, as shown in Figure 23.

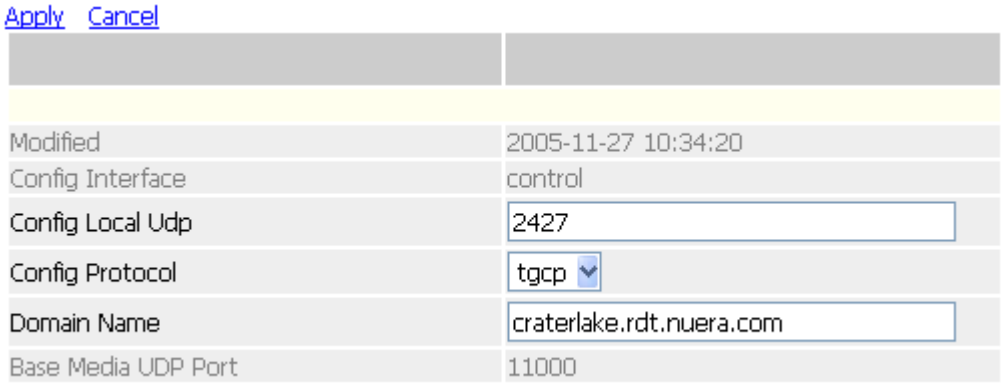


Figure 23. MGC Globals General Statistics

3. Configure **Config Local Udp** port. This is the port on which the chassis listens for call control traffic. For TGCP this value is always 2427.
4. Configure **Protocol**. This value is the call control protocol for the chassis. Currently, only **TGCP** is supported.
5. Configure the **Domain Name** (or address) to be used in TGCP messages.
6. Select **Apply**.

Configuring Remote Gateways for Force Connect Applications

Force Connect allows static connections for RTP, RTCP and T.38 transport as well as CAS and ISDN signaling transport across IP without control from a softswitch. The granularity of these connections is at the trunk level, meaning each DS1 or E1 can

have a static connection to a different BTX-4K. Static connections can only be made between like trunk types, e.g. E1 to E1.

TGCP and force connect can be mixed. Each DS1/E1 may be configured as the user sees fit (i.e. Force Connect or TGCP). The Force Connect configured endpoints will simply ignore any MGC information for the DS3/OC-3/STM-1.

You must first define a list of available remote gateways before you can establish force connections. These remote gateways define the possible destinations for all force connections created on the BTX-4K. For specific instructions on configuring Force Connect on your gateway, see page 76.

In Force Connect CAS applications, the Signal Mode should be set to bitOriented for E1 and robbedBit for T1.

MGC Configurables are not applicable to Force Connect applications.

To configure Force Connect Remote Gateways:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/ForceConnect** to display the Force Connect Information pane as shown in Figure 24.

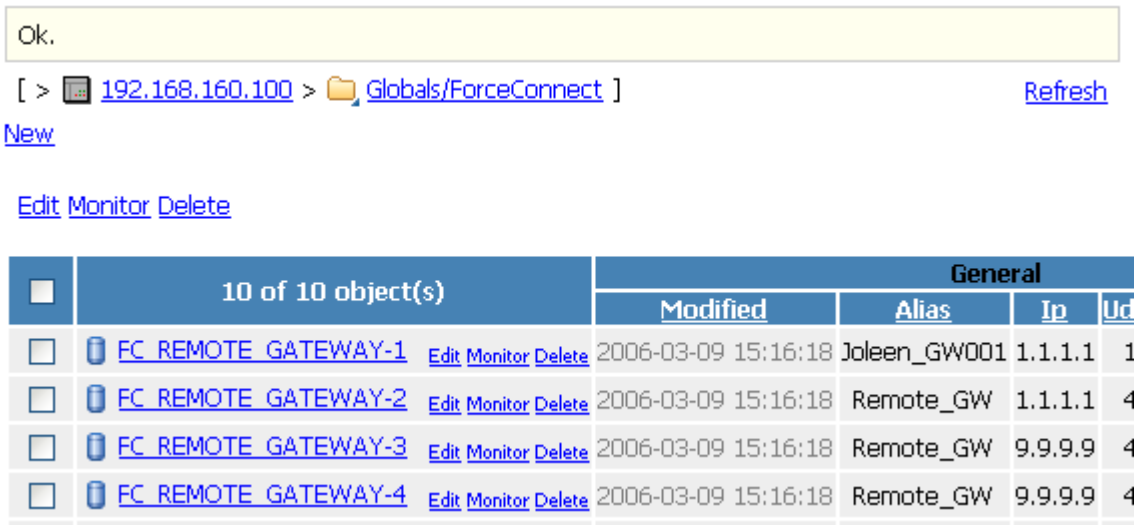


Figure 24. Force Connect Information pane

2. Select **New** from the top left or click **Edit** to the right of an existing Force Connect Remote Gateway to configure the corresponding Force Connect parameters in the Information pane, as shown in Figure 25.

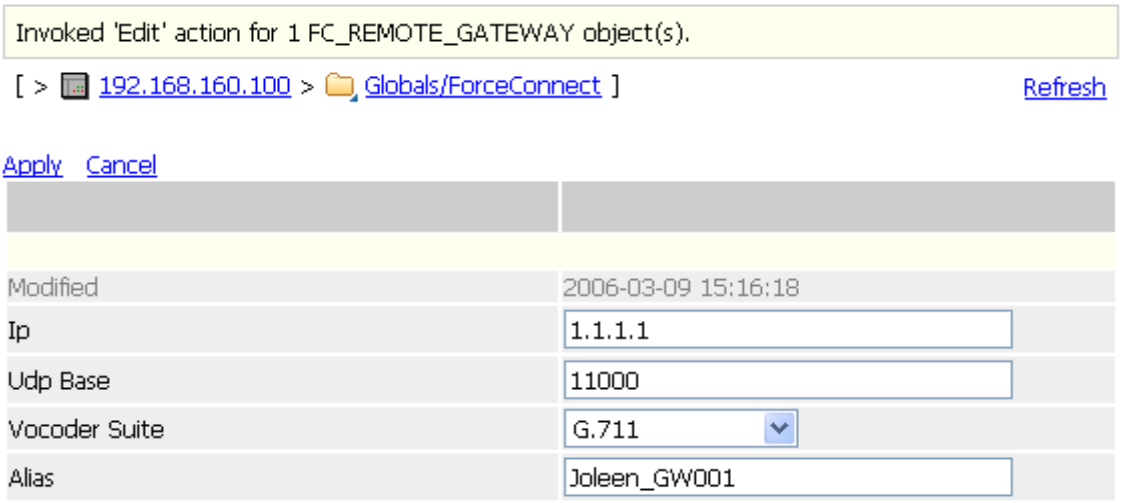


Figure 25. Force Connect Parameters

3. Enter the **IP** address of the remote gateway.
4. Enter the corresponding **UDP Base** port of the remote gateway. This is an even number between 7000 and 64128.
5. Select the appropriate **Vocoder Suite** of the remote gateway.

The Vocoder Suite is what is **configured** for the remote gateway, **not** what is authorized.

6. Enter an **Alias** for this remote gateway.
7. Select **Apply** to save your changes.

Configuring TDM Interfaces

The BTX-4K Media Gateway can be configured for DS3, STM1 and OC3 interfaces. NetConductor automatically adapts to the configuration of your BTX-4K. For example, if it detects a BTX-4K configured for metallic DS3 interfaces then you will see DS3 interfaces in the inventory of your Network Element (instead of OC-3 or STM-1).

As shown in Figure 26, a BTX-4K is said to be configured for **metallic DS3** if the VPM cards have a DS3DB module installed.

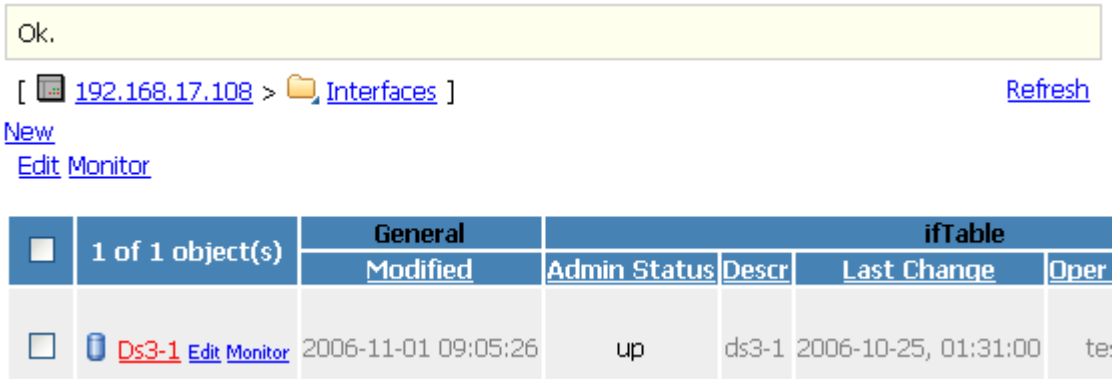


Figure 26. BTX-4K Configured for Metallic DS3

A BTX-4K is said to be configured for an **STM1** interface if the VPM cards have a OC3DB module installed and the connection type is set to STM1, as shown in Figure 27.

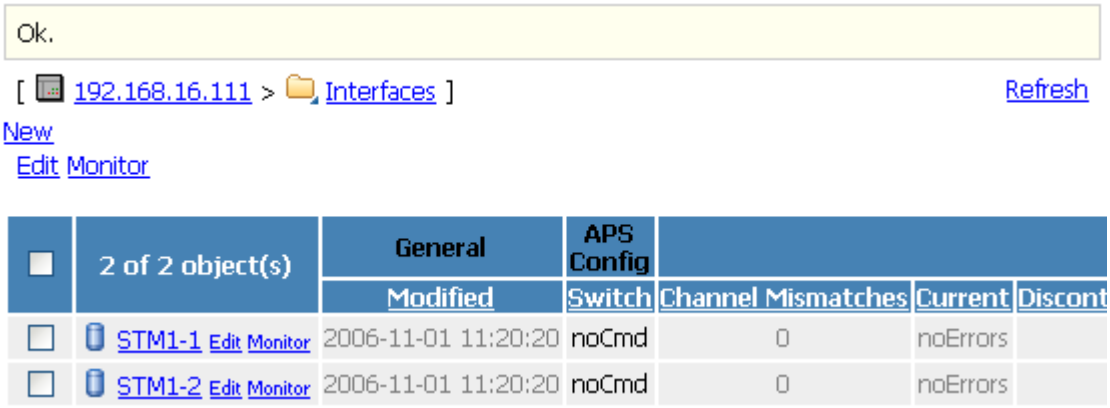


Figure 27. BTX-4K Configured for STM1 Interface

A BTX-4K is said to be configured for an **OC3** interface if the VPM cards have an OC3DB module installed and the connection type is set to OC3, as shown in Figure 28.

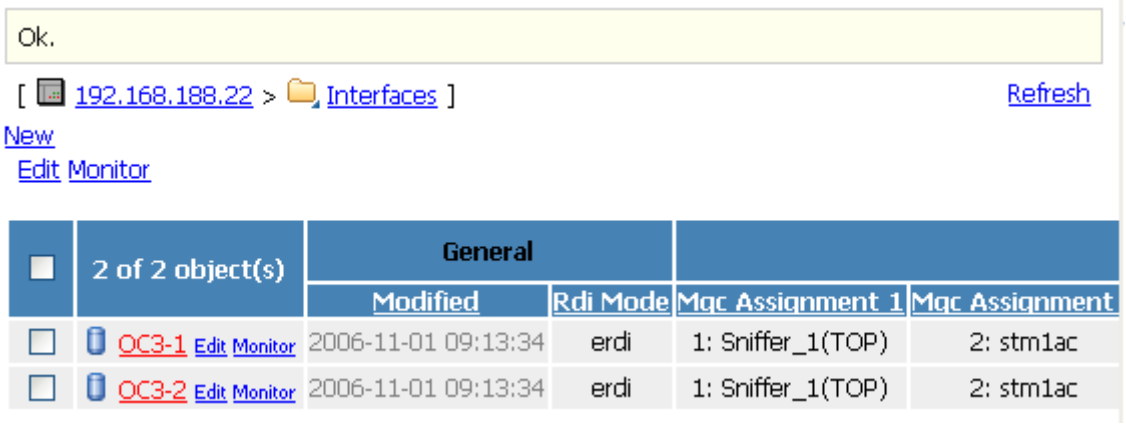


Figure 28. BTX-4K Configured for OC3 Interface .

Refer to "OC3 (SONET) DS1 and STM-1 (SDH) VC12/E1 Mapping" on page 218 for mapping OC3 to DS1s and STM-1 to VC12s.

Configuring the DS3 Interface

The DS3 interface must be manually configured in the software even if the interface is connected to an active DS3 connection. The software activates the interface and allows communication.

When configuring DS3s, the Information pane displays one long screen organized into multiple sections. For readability, the procedures that follow are broken into smaller units and may not be in the same order you see in NetConductor.

To configure the DS3 interface:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to display the Information pane shown in Figure 29.

	3 of 3 object(s)	Mgc Assignment 1	Mgc Assignment 2	Mgc Assignment 3	Mgc Assi
☐	Ds3-1 Edit Monitor	1	2	3	nc
☐	Ds3-2 Edit Monitor	none	none	none	nc

Figure 29. DS3 Information Table

2. Select the **Edit** link to the right of the DS3 you wish to configure.

The following configuration section (MGC Assignments) is only necessary when configuring TGCP Applications, not Force Connect applications.

To configure DS3s - MGC Assignments:

1. The first section allows you to configure the MGC settings as shown in Figure 30.

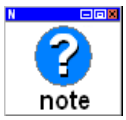
MGC	
Mgc Assignment 1	2
Mgc Assignment 2	none
Mgc Assignment 3	none
Mgc Assignment 4	none
Mgc Assignment 5	none
Mgc Assignment 6	none
Mgc Assignment 7	none
Mgc Assignment 8	none

Figure 30. DS3 MGC Information Section

2. Configure **Mgc Assignment 1**. Select the MGC template alias (and number) of the MGC to control the endpoints on the DS3.

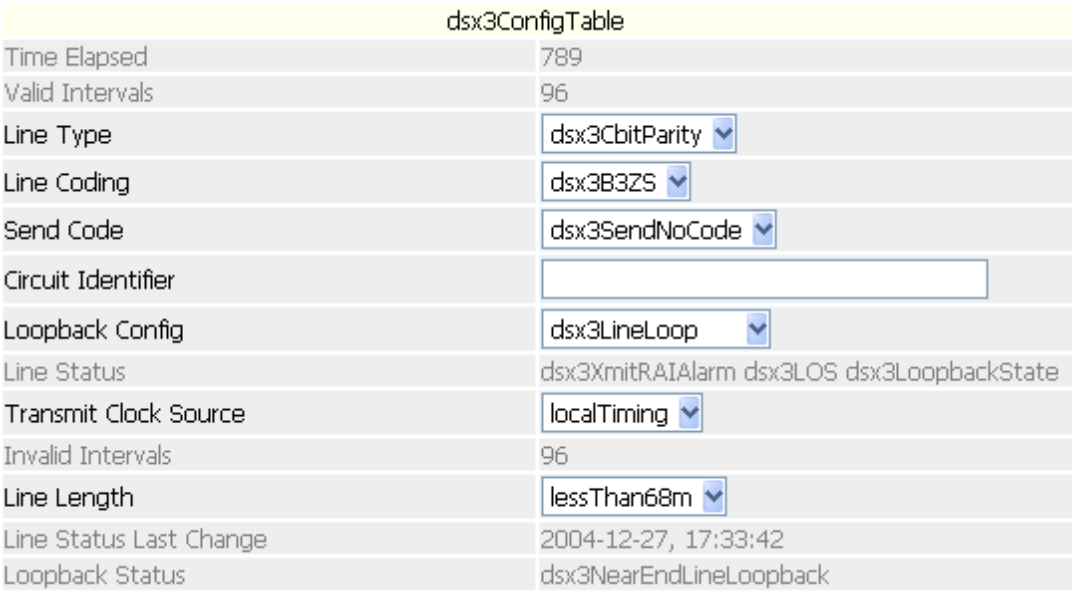
The first MGC for each DS3 will be the default MGC as defined by the Packet Cable TGCP specification. MGC 1 must be configured for proper operation of the endpoints of the DS3.

3. Optionally, configure **Mgc Assignments 2-8**.



It is not necessary for MGC Assignments to be unique to a DS3.

To configure DS3s - DS3 Config Section:



dsx3ConfigTable	
Time Elapsed	789
Valid Intervals	96
Line Type	dsx3CbitParity
Line Coding	dsx3B3ZS
Send Code	dsx3SendNoCode
Circuit Identifier	
Loopback Config	dsx3LineLoop
Line Status	dsx3XmitRAIAlarm dsx3LOS dsx3LoopbackState
Transmit Clock Source	localTiming
Invalid Intervals	96
Line Length	lessThan68m
Line Status Last Change	2004-12-27, 17:33:42
Loopback Status	dsx3NearEndLineLoopback

Figure 31. DS3 Configuration

1. Configure the **Line Type**. This is the DS3 framing format. The available options are **dsx3CbitParity** and **dsx3M13**.
2. **Line Coding** is bipolar with 3-Zero Substitution; **B3ZS** is the only option.
3. Currently, the only available option for **Send Code** is **dsx3SendNoCode**.
4. Configure the **Circuit Identifier**. This is a user-defined name not recognized by external controllers.
5. Configure the **Loopback Config**. This is a diagnostic facility with the following options:
   - The **dsx3PayloadLoop** is a DS3 subscriber loop where the loop is performed after the DS3 has been demuxed into DS1s.

- The **dsx3LineLoop** is a DS3 subscriber loop where the loop is performed before any operations are performed on the DS3.
- The **dsx3InwardLoop** is a DS3 network loop where the loop is performed after the DS3 has been muxed.
- **NoLoop** – no loopback.

6. Configure the **Transmit Clock Source**. This identifies the transmit source of the clock used by the DS3 link. The available options are:
   - **localTiming**– uses the gateway's reference clock as the transmit clock (internal clock or BITS).
   - **loopTiming** – uses the recovered receive DS3 clock source as the transmit clock source. This setting is recommended.
7. Configure the **Line Length** of the DS3 cable. If you have a long line, compensations will be made for signal degradation. Options include:
   - **Short** < 68m – default.
   - **Long** > 68m.

To configure DS3s - ifTable, mgcConfigtable, and StatsTable:

ifTable	
Descr	ds3-1
Type	ds3
Speed	44736000
Admin Status	up
Oper Status	up
Last Change	2005-11-23, 18:24:28
mgcConfigTable	
Hunt	enable
n4kIfStatsTable	
Clear	noop
Calls In Progress	289
Calls Blocked	1088
Clear Call Blocked	noop

Figure 32. DS3 ifTable and StatsTable

1. Configure the **Admin Status** to **up**. This is the desired state of DS3 physical ports.
2. Configure **Mgc Config Hunt**. When **enabled**, the MGC table will be "walked" sequentially, with the full restart procedure conducted for each DS1 until an MGC provides an ACK to the gateway. The next MGC in the list will be queried when the restart procedure times out or when a 5xx message from an MGC is received. Hunting will begin at the top of the MGC table when the last MGC in the table is unsuccessfully queried.
3. To reset (or zero) performance statistics counters for this DS3 (and DS1s under this DS3), configure **Clear** to **invoke**.

4. To **Clear Call Blocked** for this DS3, configure this parameter to **invoke**.
5. Select **Apply.**

Enabling DS1s

DS1 interfaces are applicable for a BTX-4K gateway configured for metallic DS3 or OC-3 interfaces. A DS1 object represents a VT (virtual tributary) and its contained DS1 interface. There are 28 DS1 interfaces per DS3 interface and up to 84 DS1 interfaces per OC-3 interface. Additionally, and optionally, Force Connections are made at the DS1 level. For specific instructions on enabling DS1s, see "Configuring DS1 and E1 Parameters" on page 68.

Configuring the Optical OC-3 (SONET) Interface

You can configure up to 2 OC3 interfaces in your gateway, namely OC3-1 and OC3-2. MGC assignments (up to 8 MGCs per OC3 interface) are done at the OC3 level.

To configure the OC3-1 interface:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to display a list of OC3 objects in the Information pane, as shown in Figure 33.

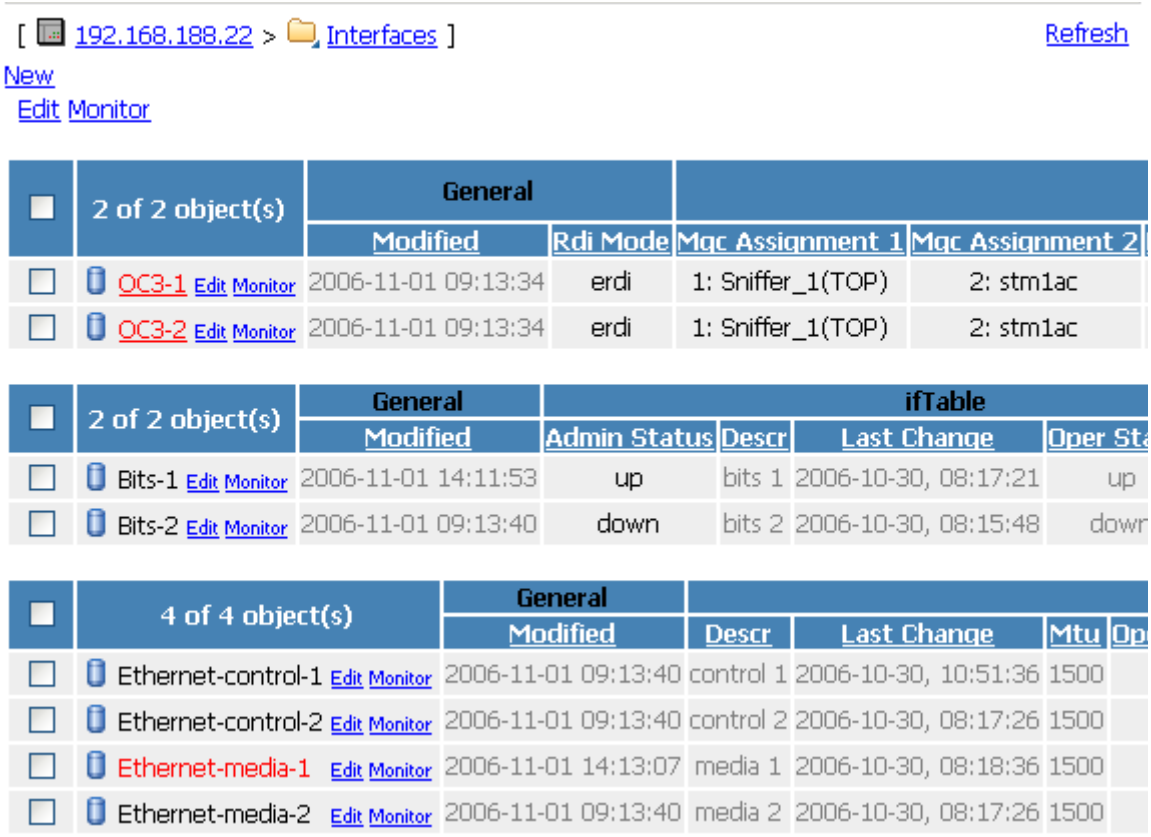
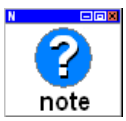

[192.168.188.22 > Interfaces]
Refresh
New
Edit Monitor
2 of 2 object(s)
General
Modified
Rdi Mode
Mgc Assignment 1
Mgc Assignment 2
OC3-1 Edit Monitor 2006-11-01 09:13:34 erdi 1: Sniffer_1(TOP) 2: stm1ac
OC3-2 Edit Monitor 2006-11-01 09:13:34 erdi 1: Sniffer_1(TOP) 2: stm1ac
2 of 2 object(s)
General
ifTable
Modified
Admin Status
Descr
Last Change
Oper St
Bits-1 Edit Monitor 2006-11-01 14:11:53 up bits 1 2006-10-30, 08:17:21 up
Bits-2 Edit Monitor 2006-11-01 09:13:40 down bits 2 2006-10-30, 08:15:48 down
4 of 4 object(s)
General
Modified
Descr
Last Change
Mtu
Ethernet-control-1 Edit Monitor 2006-11-01 09:13:40 control 1 2006-10-30, 10:51:36 1500
Ethernet-control-2 Edit Monitor 2006-11-01 09:13:40 control 2 2006-10-30, 08:17:26 1500
Ethernet-media-1 Edit Monitor 2006-11-01 14:13:07 media 1 2006-10-30, 08:18:36 1500
Ethernet-media-2 Edit Monitor 2006-11-01 09:13:40 media 2 2006-10-30, 08:17:26 1500

Figure 33. OC3 Interface Objects

2. Select **Edit** to the right of the **OC3-1** to open the configurable parameters in the Information pane, as shown in Figure 34.



MGC Configurables are not applicable to Force Connect applications.

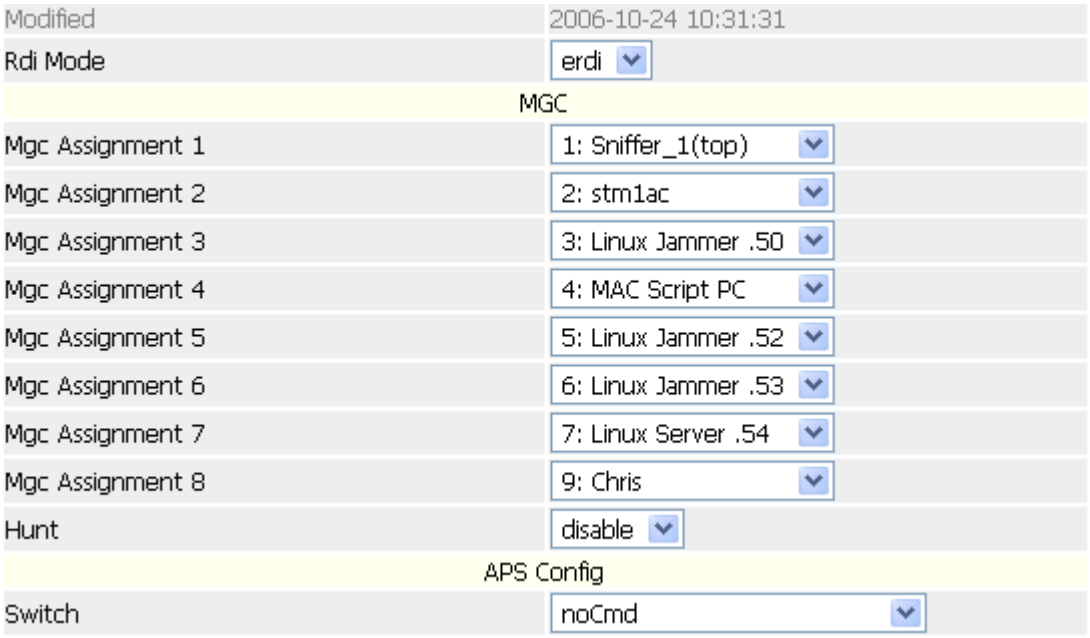


Figure 34. OC-3 Configurable Parameters

3. Configure **Rdi Mode**. Choose between **standard** and **enhanced** mode for Remote Defect Indication for the STS-1 path and virtual tributary. The default is **erdi** mode.
4. Configure **Mgc Assignment 1**. These assignments are made at the OC-3 interface level.
5. Optionally, configure **Mgc Assignments 2-8**.

It is not necessary for MGC Assignments to be unique to a OC-3.

6. Configure **Mgc Config Hunt**. When **enabled**, the MGC table will be "walked" sequentially, with the full restart procedure conducted for each DS1 until an MGC provides an ACK to the gateway. The next MGC in the list will be queried when the restart procedure times out or when a 5xx message from an MGC is received. Hunting will begin at the top of the MGC table when the last MGC in the table is unsuccessfully queried.
7. Set **Switch** to force a switch of the **Working** and **Protect** interface.
8. Select **Apply** to save your changes.

OC-3 Working and Protect Interface

A BTX-4K configured for **optical OC-3** contains two OC-3 interfaces: the OC3-1 and OC3-2. In turn, each of these interfaces has a Working and Protect interface. Namely **OC3-1/APSGroup-Working-1** and **OC3-1/APSGroup-Protect-1**. All statistics are collected at this interface level.

To configure the OC3-1 Working:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **OC3-1** to display the Information pane shown in Figure 35.

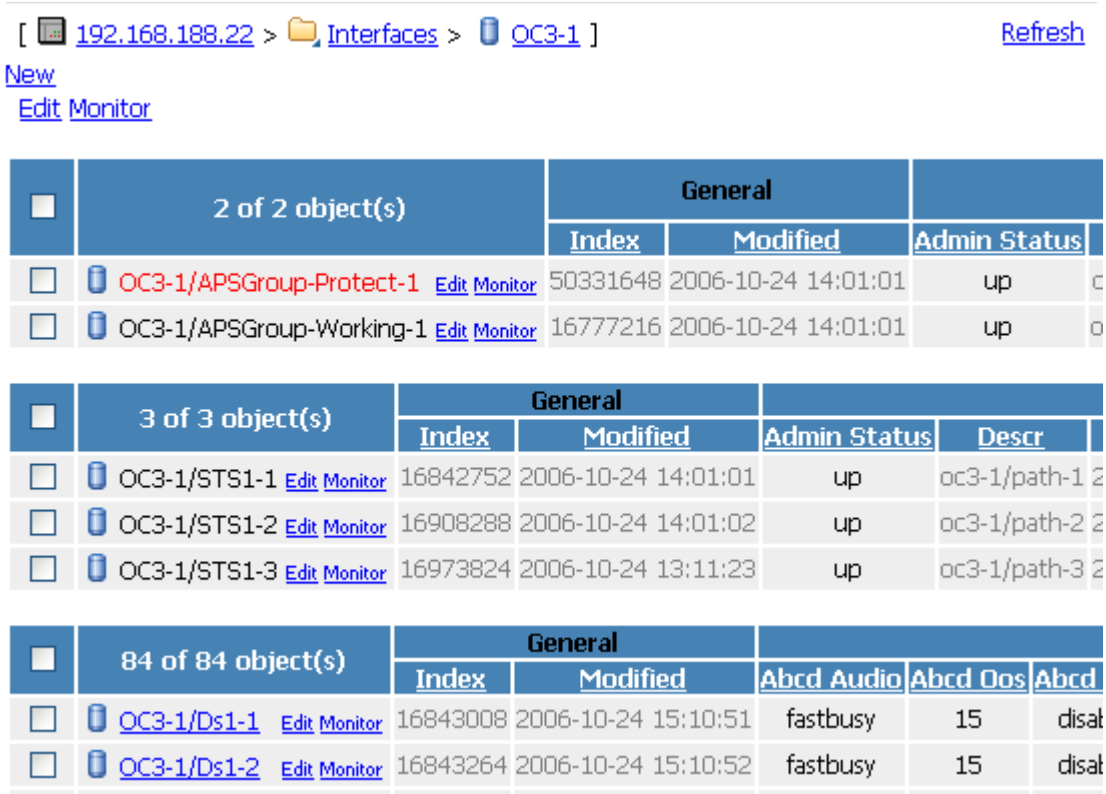


Figure 35. OC3-1 Interface Objects

2. Select **Edit** to the right of **OC3-1/APSGroup-Working-1** to display the OC-3 Information pane, as shown in Figure 36.

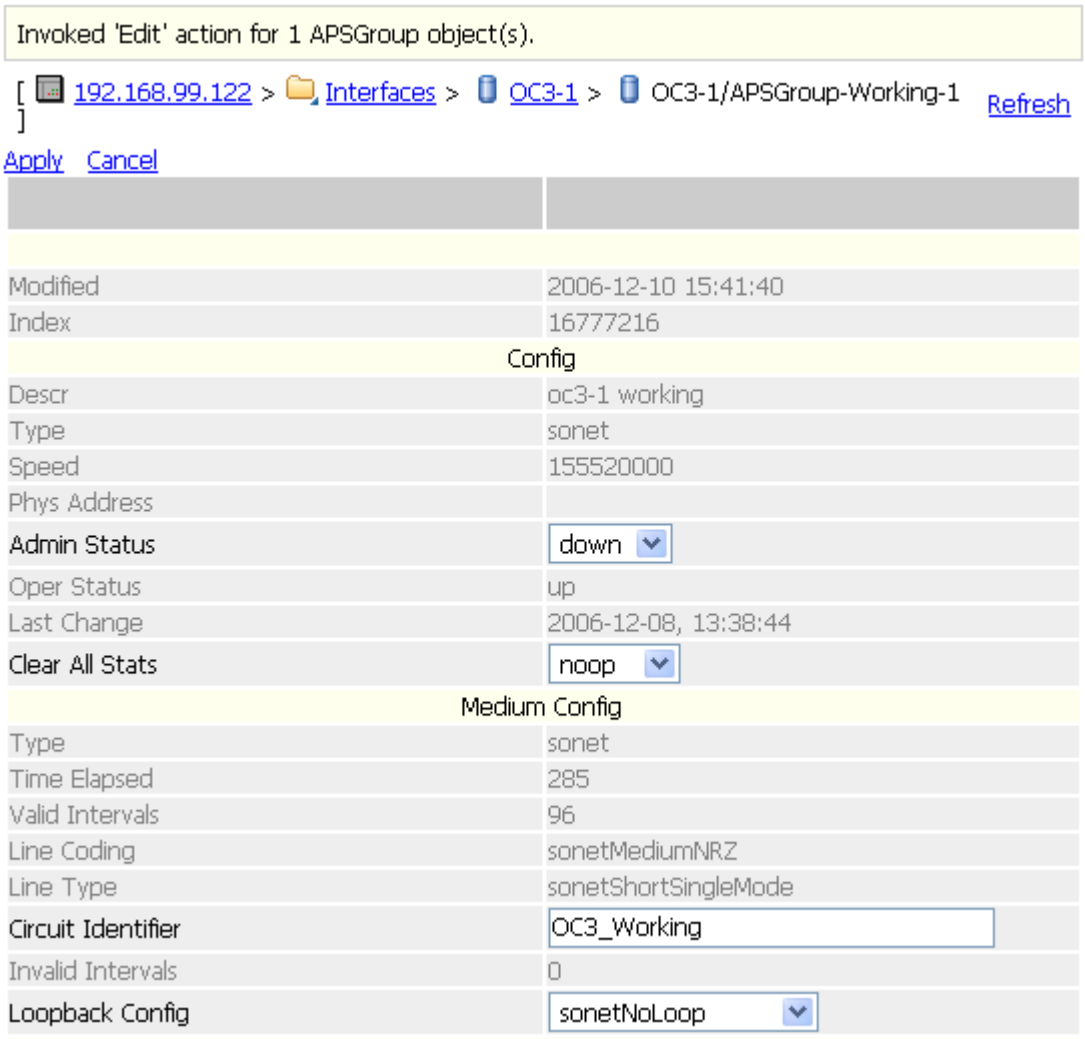


Figure 36. OC3-1 Working Interface Parameters (cropped)

3. Set **Admin Config** to **up** to enable this interface.
4. To **Clear All Stats** for this OC-3, configure this parameter to **invoke**.
5. Optionally enter a **Circuit Identifier** to give this interface a name.
6. Configure the OC-3 **Loopback Config** from the drop-down menu. This is a diagnostic facility with the following options:
   - The default value is **sonetNoLoop**.
   - **SonetFacilityLoop** specifies that the received signal at this interface is looped back out through the corresponding transmitter in the return direction.
   - **SonetTerminalLoop** ensures the signal about to be transmitted is connected to the associated incoming receiver.
7. Select **Apply** to save your changes.

8. Repeat these steps for the **OC3-1 Protect interface**.

Enabling the STS-1 Interface

STS-1 interfaces are only applicable for a BTX-4K configured with a SONET OC3 interface. The gateway includes 3 STS-1 interfaces for each OC3, for a total of 6 STS-1 interfaces per gateway. There are no 24-hour statistics counters collected for STS-1 interfaces.

To enable an STS-1:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **OC3-1** to display the Information pane shown in Figure 37.

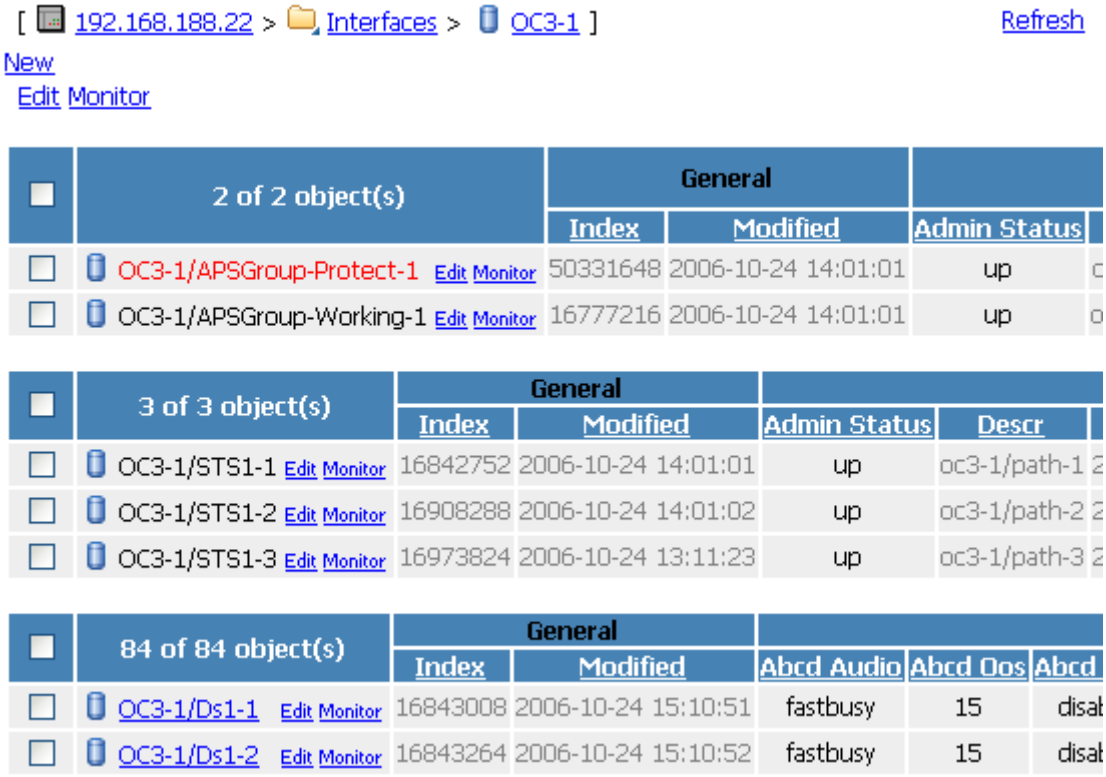


Figure 37. STS-1 Interface Objects

2. Select **Edit** to the right of the **OC3-1/STS1-1** to display the STS-1 configuration parameters in the information pane, as shown in Figure 38.

Figure 38. STS-1 Configuration Parameters

3. Set **Admin Status** to **up** to enable this interface.
4. To clear the stats for this STS-1, invoke **Clear All Sonet Stats**.
5. To **Clear Call Blocked** for this STS-1, configure this parameter to **Invoke**.
6. Optionally enter a **Circuit Identifier** to give this interface a name.
7. Select **Apply** to save your changes.

Configuring the Optical STM-1 (SDH) Interface

To configure the STM1-1 interface:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to display a list of Interfaces in the Information pane, as shown in Figure 39.

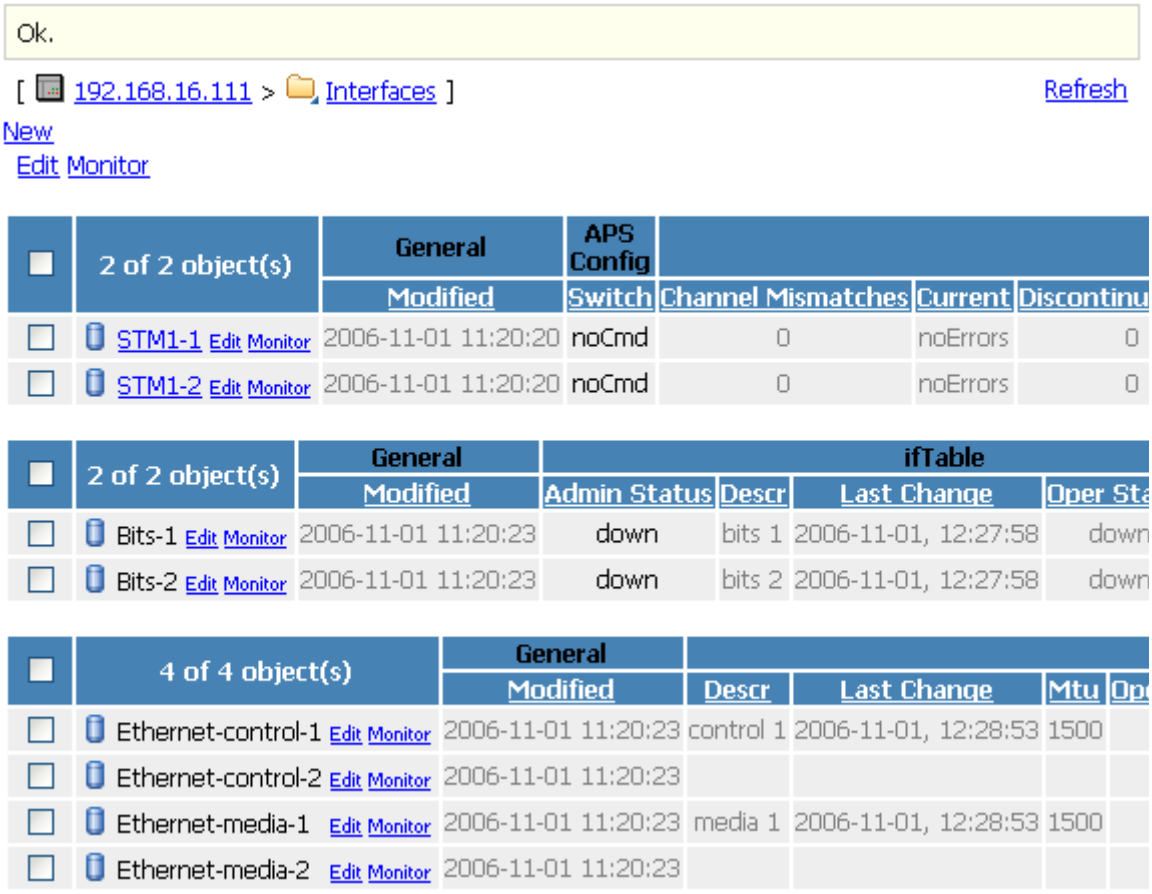


Figure 39. STM-1 Interface Objects

2. Select **Edit** to the right of the STM-1 to open the configurable parameters in the Information pane, as shown in Figure 40.

MGC Configurables are not applicable to Force Connect applications.

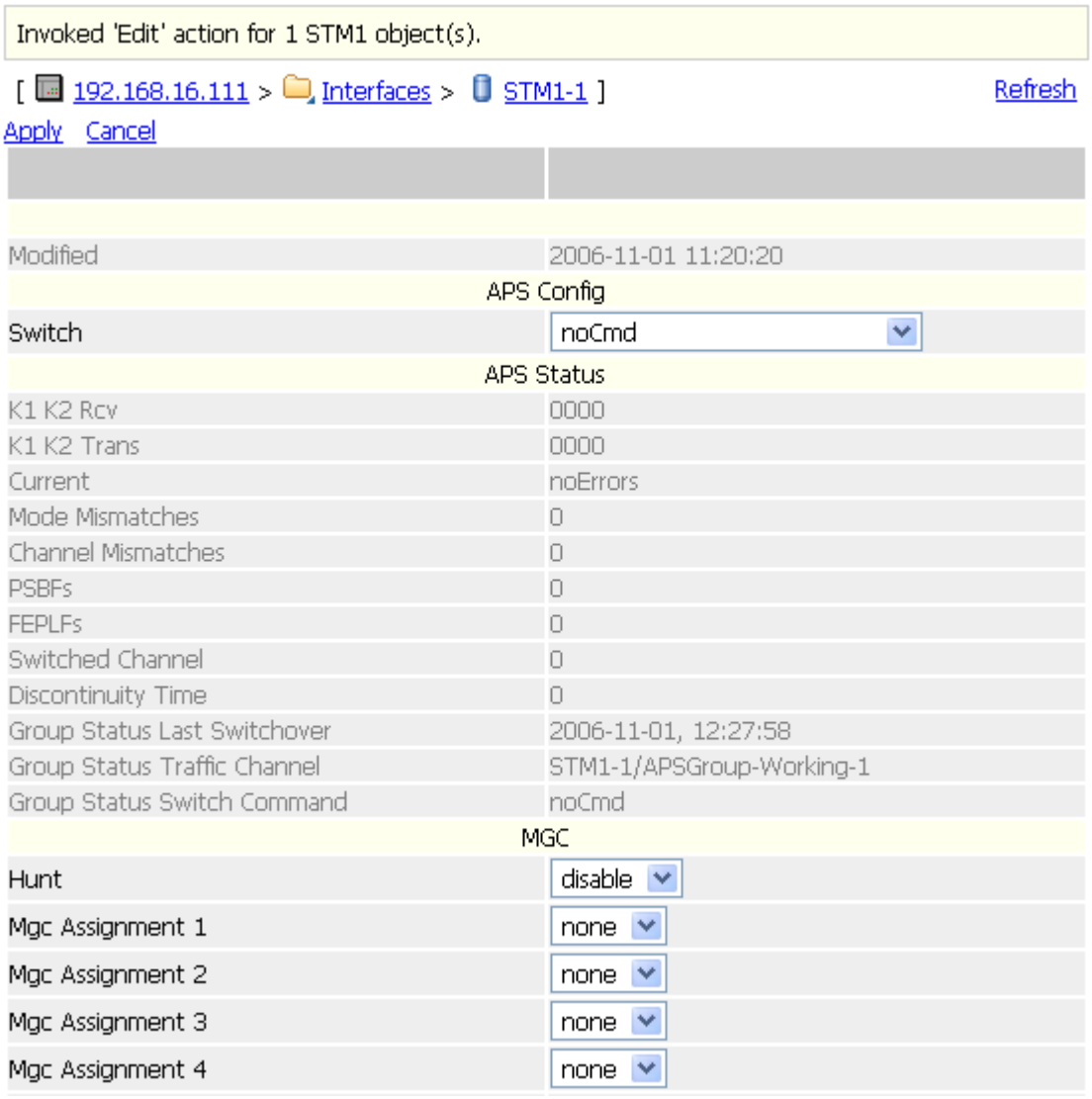


Figure 40. STM-1 Configurable Parameters

3. Configure the **Switch** drop-down menu to force a switch of the **Working** and **Protect** interface.
4. Configure **Mgc Assignment 1**. MGC assignments are made at the STM-1 interface level.
5. Optionally, configure **Mgc Assignments 2-8**.

It is not necessary for MGC Assignments to be unique to a STM-1.

6. Configure **Mgc Config Hunt**. When **enabled**, the MGC table will be "walked" sequentially, with the full restart procedure conducted for each E1 until an MGC provides an ACK to the gateway. The next MGC in the list will be queried when the restart procedure times out or when a 5xx message from an MGC is received. Hunting will begin at the top of the MGC table when the last MGC in the table is unsuccessfully queried.
7. Select **Apply** to save your changes.

STM-1 Working and Protect Interface

A BTX-4K configured for **optical STM-1** contains two STM-1 interfaces: the STM1-1 and STM1-2. In turn, each of these interfaces has a Working and Protect interface. Namely **STM1-1/APSGroup-Working-1** and **STM1-1/APSGroup-Protect-1**. All statistics are collected at this interface level. You should follow the configuration process detailed here for both interfaces.

To configure the STM1-1 Working Interface:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **STM1-1** to display the Information pane shown in Figure 41.

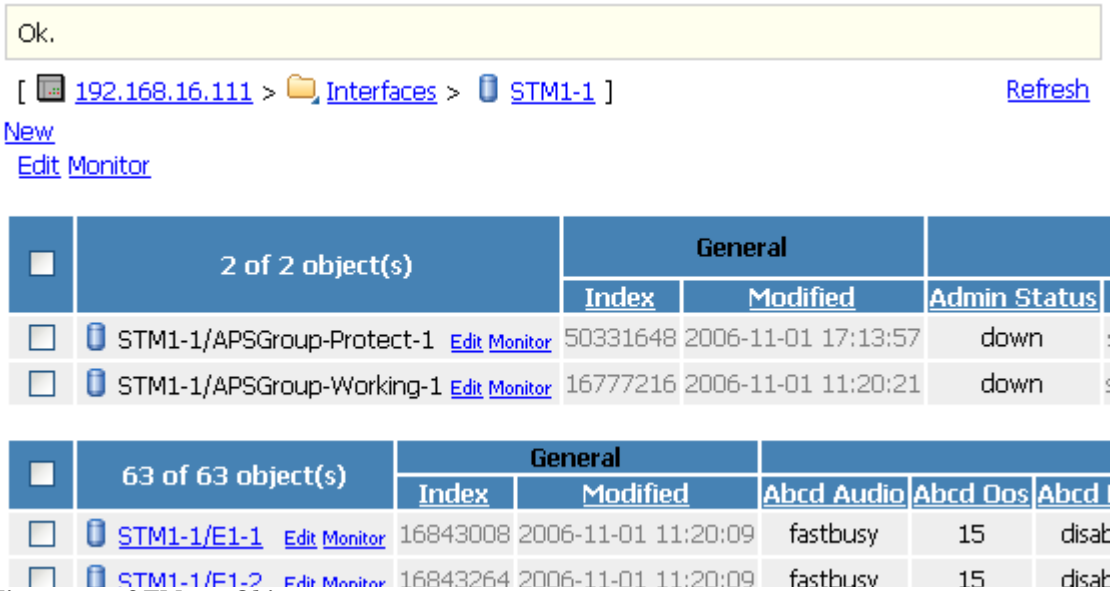


Figure 41. STM-1-1 Objects

2. Select **Edit** to the right of the **STM1-1/APSGroup-Working** Interface to display the STM-1 Information pane, as shown in Figure 42.

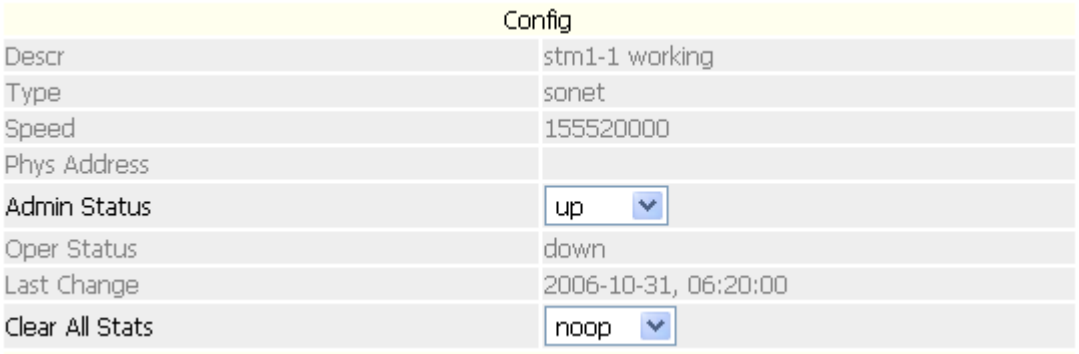


Figure 42. STM-1 Working Interface Parameters (cropped)

3. To **Clear All Stats** for this OC-3, configure this parameter to **invoke**.
4. Optionally enter a **Circuit Identifier** to give this interface a name.

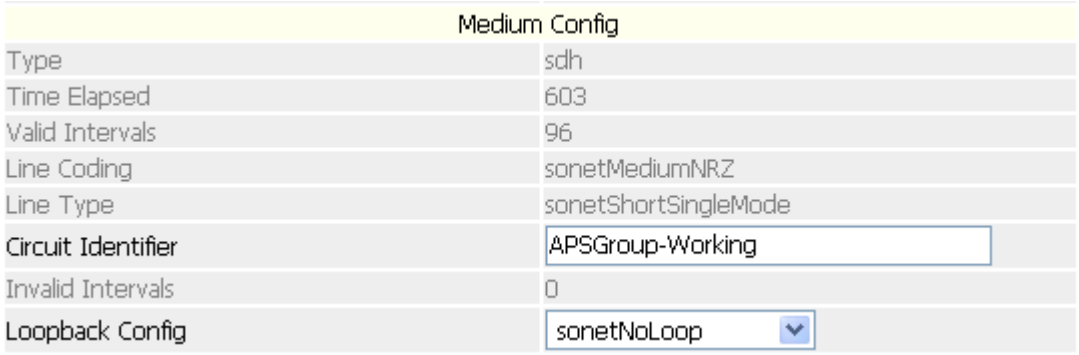


Figure 43. STM-1 Working Interface parameters (cropped)

5. Configure the STM-1 **Loopback Config** from the drop-down menu:
   - The default is **sonetNoLoop**.
   - **SonetFacilityLoop** specifies that the received signal at this interface is looped back out through the corresponding transmitter in the return direction.
   - **SonetTerminalLoop** ensures the signal about to be transmitted is connected to the associated incoming receiver.
6. Set **Admin Config** to **up** to enable this interface.
7. Select **Apply** to save your changes.
8. Repeat these steps for the **STM-1 Protect interface** before continuing.

Enabling VC4s

To enable a VC4:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **STM1-1** to display the VC4 object in the Information pane, as shown in Figure 45.

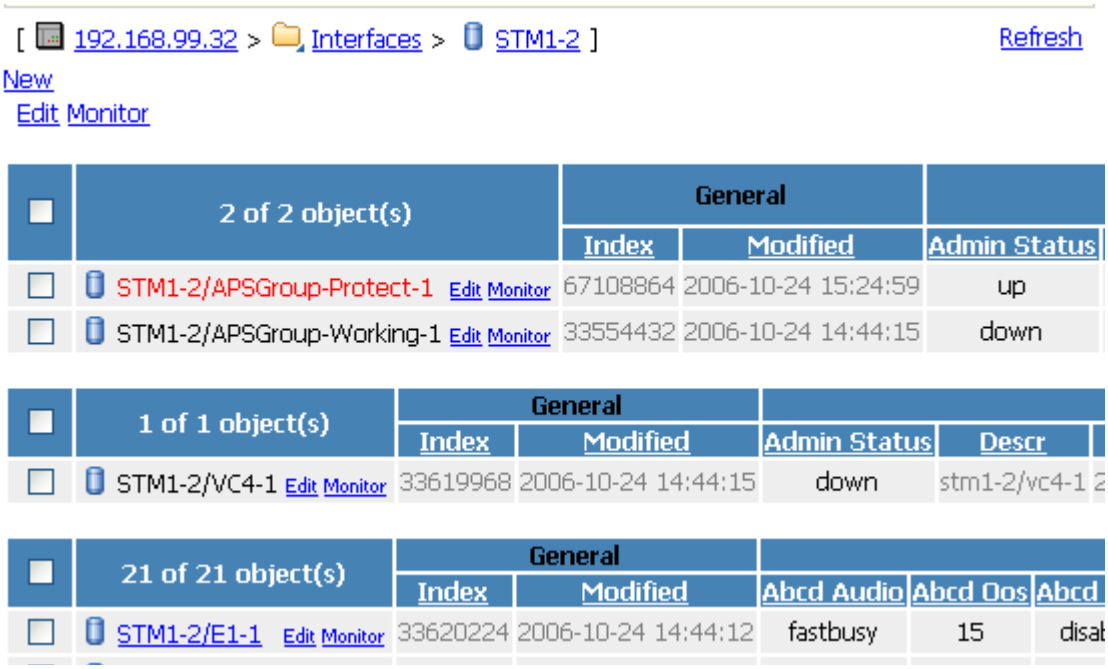


Figure 44. VC4 Interface Information Pane

2. Select Edit to the right of the VC4 to display the VC4 configuration parameters in the information pane, as shown in Figure 45.

Figure 45. VC4 Configuration Parameters

3. Set **Admin Config** to **up** to enable this interface.
4. To clear the stats for this VC4, invoke **Clear All Sonet Stats**.
5. To **Clear Call Blocked** for this VC4/STM-1, configure this parameter to **Invoke**.
6. Optionally enter a **Circuit Identifier** to give this interface a name.
7. Select **Apply** to save your changes.

Enabling E1s

E1 interfaces are only applicable for a BTK-4K gateway configured for STM-1 interfaces. A E1 object represents a VC (virtual container) and its contained E1 interface. There are 63 E1 interfaces per STM-1 interface, for a total of 126 E1 interfaces per BTX-4K, namely: STM1-1/E1-1 through STM1-2/E1-63. Force Connect configurations are made at the E1 level.

Configuring DS1 and E1 Parameters

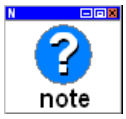
This section details the configuration of both DS1 and E1 interfaces contained within DS3, OC-3 (SONET), or STM-1 (SDH) interfaces. For simplicity, throughout this section, E1 interfaces will be referred to as DS1 interfaces.

The software activates the interface and allows communication, so you must configure the DS1 in NetConductor before proceeding. DS0s associated with a DS1 are configured globally by the settings of the DS1.

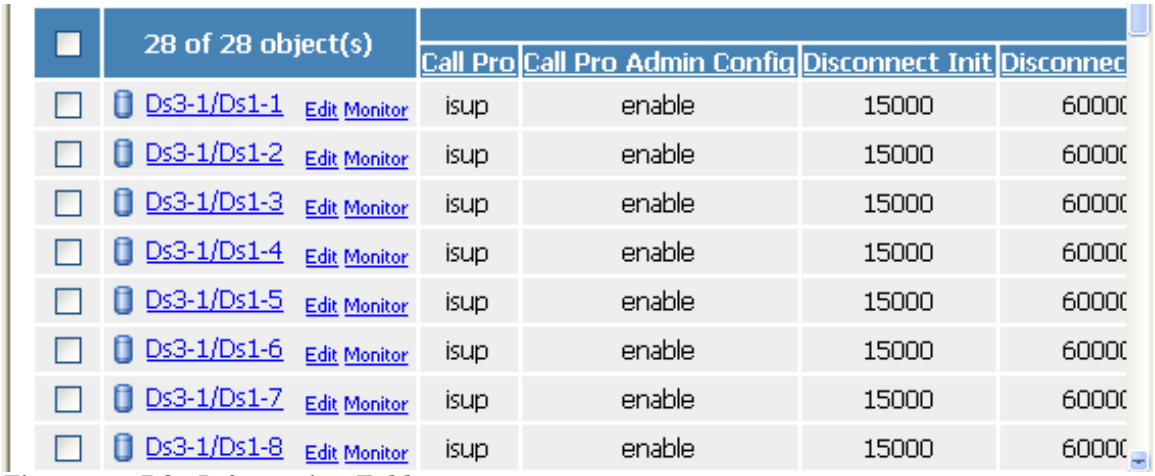
When displaying DS1 or E1 configuration parameters, the NetConductor Information pane presents one long screen organized into multiple sections. For the sake of readability, these parameters are presented in shorter procedural pieces and the screens shown here may omit non-configurable statistics you will see in NetConductor.

To enable a DS1 interface:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **DS3-n** to display the Information pane shown in Figure 46.



In NetConductor, DS1s are located under the corresponding TDM Interface. If your gateway is configured for STM1, expand the hierarchy by selecting **Inventory > [NE] > Interfaces > STM1-1**. For an OC3 configured gateway, **Inventory > [NE] > Interfaces > OC3-1**.



28 of 28 object(s)	Call Pro	Call Pro Admin Config	Disconnect Init	Disconnec
Ds3-1/Ds1-1 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-2 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-3 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-4 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-5 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-6 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-7 Edit Monitor	isup	enable	15000	60000
Ds3-1/Ds1-8 Edit Monitor	isup	enable	15000	60000

Figure 46. DS1 Information Table

2. Click **Edit** to the right of the DS1 to configure.

To configure DS1s - Media Section:

1. The first section, shown in Figure 47, allows you to configure the Media settings.

Media	
Gain Enc	0
Gain Dec	0
Voice Codec	pcmUlaw64k10ms
Echo Enable	enabled
Echo Nlp Enable	enabled
Echo Tone Disabler	enabled
Vad Enable	none
Vad Threshold	-36
Vad Hangover	255
Compand	pcmUlaw
Fax Codec	none
Modem Codec	none
RFC2833 Payload	127
Dtmf Relay	enabled
Digit Level	-7
Abcd Relay	disabled
Abcd Oos	15
Abcd Audio	silence
Abcd Trans Enc	0123456789abcdef
Abcd Trans Dec	0123456789abcdef

Figure 47. DS1 Media Configuration Section

Configuration parameters marked with an asterisk (*) are default values and can be overridden by parameters sent in TGCP messages from the MGC. If the MGC does not send a parameter, the default parameter is used.

2. Configure **Gain Enc**. This is the encoding gain level for the media channel at the input of the encoder in dBm0. Valid values are integers between -16 and 7.
3. Configure **Gain Dec**. This is the decoding gain level for the media channel at the output of the decoder in dBm0. Valid values are integers between -16 and 7.
4. Configure **Voice Codec***. This value sets the voice codec and packetization

period defaults. Choose from: PCM μ law, PCM A-law (10, 20, 30ms packet period) and G.729A (10, 20, 30, 40, 50, 60ms packet period).

Although G.729A is always selectable, it only works when G.729A vocoder authorization files are installed on the gateway.

5. Configure **Echo Enable***. This value controls the default state of the echo canceller. When enabled, the echo canceller cancels any echo present on the line.
6. Configure **Echo Nlp Enable**. This value controls the echo canceller's non-linear processor, which is used to further suppress any residual echo.
7. Configure **Echo Tone Disabler**. This value controls the echo canceller's tone disabler, which automatically disables the echo canceller when modem tones are detected.
8. Configure **Vad Enable***. This setting controls the voice activity detector. It can be set to adaptive (VAD adaptively determines the difference between voice and background noise), fixed (VAD decision is based on configured level threshold and hangover), or none. When enabled, the VAD blocks the transmission of packets when voice is not present.
9. Configure **Vad Threshold**. This is for fixed Vad mode only and is expressed in dBm0. This specifies the fixed signal level threshold the fixed Vad uses to make the decision between voice and silence. Note that the Vad hangover timer activates when the signal drops below this level. If the Vad hangover time expires before the signal level rises above this threshold, packet transmission stops.
10. Configure **Vad Hangover**. This is for fixed Vad mode only. This value is measured in milliseconds, and specifies the amount of time that the signal can remain below the Vad threshold before packet transmission will stop.
11. Configure **Compand**. This value controls the companding type to be used on the DS0s for this DS1. Use either μ law or A-law. Note that this only controls the format used for the channels on the DS1 side. It is **not** related to the voice codec.
12. Configure **Fax Codec**. This is the codec used upon fax modem detection. If set to **none**, no automatic codec switch occurs when fax tones are detected. **Fax Codec** can be set to **none**, **t38onV21** or **t38onv21andCng**.
13. Configure **Modem Codec**. This is the codec to use upon modem signal detection. If this is set to **none**, no automatic codec switch will occur when modem tones are detected. Choose from **none**, **pcmUlaw**, and **pcmAlaw**.
14. Configure **RFC2833 Payload**. This is the RTP payload type value for RTP packets carrying RFC2833 payloads. This is only applied when DTMF or ABCD relay is set to enable.
15. Configure **Dtmf Relay**. This is the DTMF signaling relay. When enabled, DTMF is transported via RFC2833. Nuera recommends enabling this option if a low bit rate voice codec has been selected.
16. Configure **Digit Level**. This is for DTMF digits. This field describes the power

level of the tone, expressed in dBm0, sent toward the subscriber.

17. Configure **Abcd Relay**. This is the ABCD signaling relay used to transport CAS signaling bits via RFC2833. This configuration is applicable only on force connect trunks such that CAS information can be sent end to end.
18. Configure **Abcd Oos**. This is the ABCD CAS bit pattern to generate on each channel when the trunk has a call pro admin status of disable.
19. Configure **Abcd Oos Audio**. This is the audio pattern to generate on each channel when the trunk has a call pro admin status of disable.
20. Configure **Abcd Trans Enc**. This configuration allows you to translate incoming CAS bit patterns.
21. Configure **Abcd Trans Dec**. This configuration allows you to translate outgoing CAS bit patterns.

To configure DS1s - Media TGCP Section:

1. The second section, shown in Figure 48, allows you to configure the Media TGCP settings.

Media TGCP	
Call Pro Admin Config	disable
Call Pro	isup
Ip Tos	160
Initial Resend Delay	200
Max Resend Delay	5000
Hunt Resend Count	3
Disconnect Retransmits	10
Disconnect Init	15000
Disconnect Max	60000
Wildcard Rsip Enable	enabled
Piggyback Response Enable	enabled
Encryption Enable	enabled
Retransmit Timer Max	20000
Response History Length	30000
Xgcp Feature Config	0

Figure 48. DS1 Media TGCP Configuration Section

Configuration parameters marked with an asterisk (*) are default values and can be overridden by parameters sent in TGCP messages from the MGC. If the MGC does not send a parameter, the default parameter is used.

2. Configure the **Call Pro Admin Config** to **Enable**. This is the administrative configuration of the channel for communicating with MGCs. When enabled, the channel processes TGCP or, for force connections, will go to the active state of the connection. This configuration also allows you to block the channels. When disabled, the channels will ignore all TGCP messages or, for force connections, will go to the inactive state of the connection.

You must enable Call Pro Admin Config to process TGCP or establish Force Connections.

3. Configure **Call Pro**. The call processing protocol options for the media channel are:
   - **isup**, for SS7, which is the default value. Note that Signal Mode must be con-

figured to *none* on the DS1 for this to work. This isup Call Pro setting is also used for ISDN trunks (FAS and NFAS) that utilize ISDN backhaul over IUA/SCTP (see "Configuring IUA" on page 84 for more information).

- **mo**, for Emergency 911 services. Note that Signal Mode must be configured to *robbedBit* on the DS1 for this to work.
- **mt**, for Busy Line Verification and Operator Interrupt. Note that Signal Mode must be configured to *robbedBit* on the DS1 for this to work.
- **forceConnect** for bearer only channels (i.e. ISUP CIC trunks or CAS trunks).
- **forceConnectPRI** for signaling and bearer channels (i.e. ISDN PRI trunks).

4. Configure **Ip Tos***. This is the type of service value in the IP header for media packets and should be entered as a decimal value between 0 and 255.
5. Configure **Initial Resend Delay**. This is the elapsed time before the first resend of a TGCP message.
6. Configure **Max Resend Delay**. This is the maximum resend delay for TGCP messages.
7. Configure **Hunt Resend Count**. This is the number of TGCP resends before the endpoint tries the next resolved IP address of the current notified entity, if one exists. If there is only one resolved IP address for the current notified entity, this configuration does nothing unless MGC Hunt is enabled, then it goes to the next MGC on the list.
8. Configure **Disconnect Retransmits**. This is the total number of retransmits of a given TGCP message before the disconnected procedure is initiated.
9. Configure **Disconnect Init**. This is the maximum delay before entering the TGCP disconnected procedure.
10. Configure **Disconnect Max**. This is the maximum delay between successive TGCP disconnected procedures when fully backed off.
11. Configure **Wildcard Rsip Enable**. When enabled, this allows the gateway to send a single RSIP for multiple channels. For example, there is one RSIP for all DS0s of a DS1. When disabled, individual RSIPs for each port will always be sent.
12. Configure **Piggyback Response Enable**. This configuration enables or disables piggybacking for TGCP messages.
13. Configure **Encryption Enable***. This setting controls the default setting for media encryption. Note that even when this is set to disable, full security negotiations will be performed and the media channel will run encryption if the MGC specifies a security ciphersuite in the LCO of a TGCP message. This encryption is not applicable for Force Connections.
14. Configure **Retransmit Timer Max**. Set the time when retransmissions for a command cease. Associated with TsMax in the TGCP protocol. The default value is **20000** ms.
15. Configure **Response History Length**. Set the lifetime of a given TGCP transaction ID. The default value is **30000 ms**.

16. **Xgcp Feature Config** is a bitmap reserved for the enabling and disabling of TGCP call processing features. Setting this to **1** will trigger a DLCX on the RTCP timeout. For the default value of 0, this RTCP timeout is ignored. The current timeout is 30 minutes.

To configure DS1s - DS1 Config Section:

1. The next section, shown in Figure 49, allows you to configure the DS1 settings.

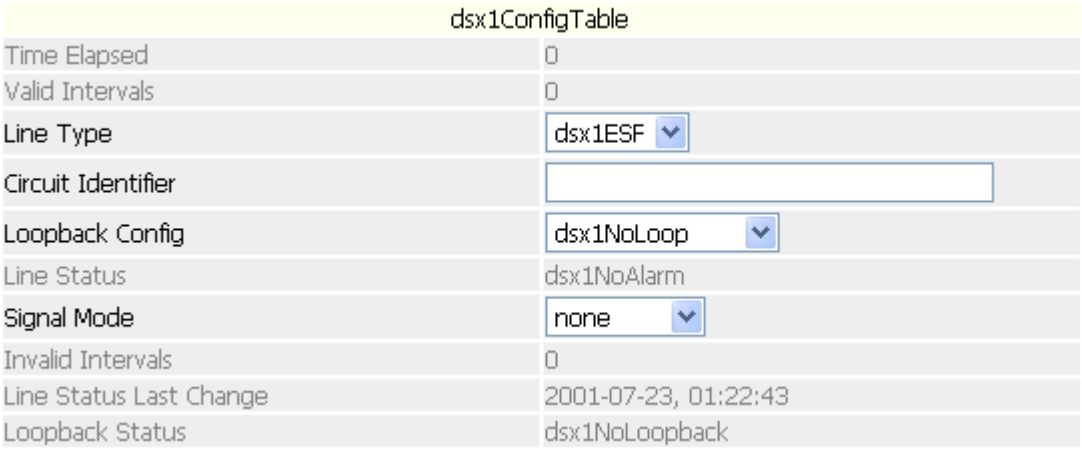


Figure 49. DS1 Configuration Section

2. Configure the **Line Type**. This parameter indicates the variety of DS1 or E1 application implemented on this interface. The valid options are:
   - **dsx1ESF (DS1 only)** – default framing format**.**
   - **dsx1D4 (DS1 only)**
   - **dsx1E1 (E1 only)**
   - **dsx1E1CRC (E1 only)**
3. Configure the **Circuit Identifier**. This is a user-defined field. For OC-3 or STM-1 interfaces this field is used as the DS1/E1 path trace label (J2 byte) which can be used by external controllers for path trace confirmation. For DS1s within a DS3 interface this field is not recognized by external controllers
4. Configure the **Loopback Config**. This is a diagnostic facility with the following options:
   - **No loopback**
   - **dsx1LineLoop** – data received on DS1 at the BTX-4K is looped back out to the line.
   - **dsx1InwardLoop** – data sent from the BTX-4K to the DS1 is looped back in to the BTX-4K.
5. Configure Signal Mode. For DS1, two options are available: none and robbedBit. Use none for ISUP (SS7) controlled DS1s. Use robbedBit for MF Controlled (Emergency 911, Operator Services, etc.) DS1s. For E1, choose between none and

bitOriented.

To Configure DS1s - MediaTones:

1. The **MediaTones** section allow you to configure the MediaTones for **busy**, **dialtone**, **fastbusy**, **ringback**, and **warble**. The configurables for each MediaTone type is the same and are shown in Figure 50.

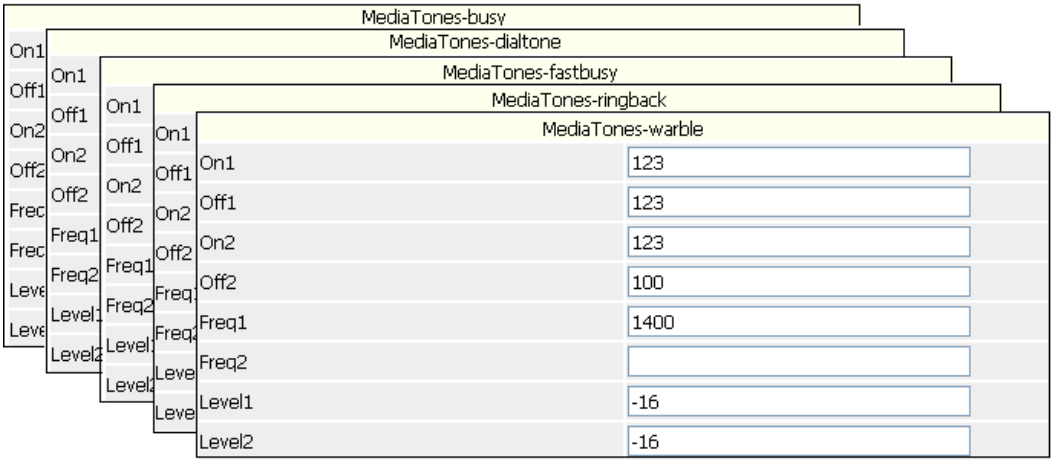


Figure 50. MediaTones Sections

1. The On1, Off1, On2, Off2 times define the cadence of the call progress tone.
2. **On1** is the amount of time, in ms, of the first “on” interval of the cadence. During this time, both configured frequencies will be generated at their configured level.
3. **Off1** is the amount of time, in ms, of the first "off" interval of the cadence. During this time, silence will be generated.
4. **On2** is the amount of time, in ms, of the second "on" interval of the cadence. During this time both configured frequencies will be generated at their configured level.
5. **Off2** is the amount of time, in ms, of the second "off" interval of the cadence. During this time, silence will be generated. The off2 interval is followed by the on1 interval and the cadence repeats.
6. **Freq1** and **Freq2** identify the frequency of the tones. This parameter is measured in Hz.
7. **Level1** and **Level2** indicate the level (volume) of the tones in dBm0.

To configure Force Connect on a DS1:

1. Near the bottom of the screen DS1 Information pane, as shown in Figure 51, you can now enable Force Connect on a trunk level.

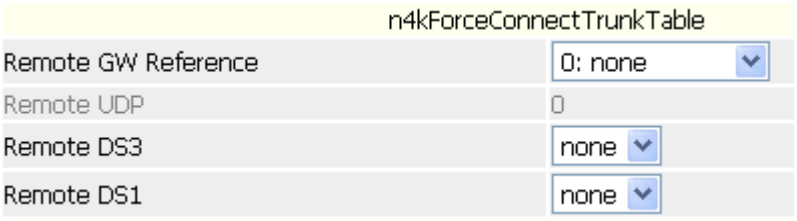


Figure 51. Force Connect Parameters on a DS1 Trunk

2. Enter the **Remote GW Reference**. This is the Alias (and number) of one of the remote gateways defined in the Force Connect Remote Gateway Table.
3. Enter the **Remote DS3 (or STM1)** to select the desired DS3 (or STM1) on the remote gateway.
4. Enter the **Remote DS1 (or E1)** to select the desired DS1 (or E1) on the remote gateway.

Force connect is not supported in OC3.

To configure DS1s - ifTable and StatsTable:

1. The third section, shown in Figure 52, allows you to configure the DS1 settings.

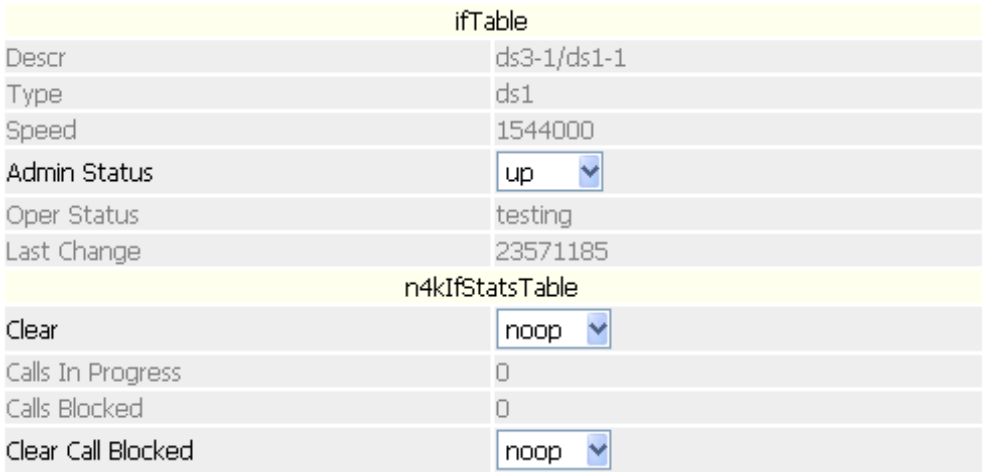


Figure 52. DS1 ifTable and StatsTable Section

2. Configure **Admin Status** to **up**. This is the desired state of DS1 physical ports.
3. To reset (or zero) performance statistics counters for this DS1, configure **Clear** to **invoke**.
4. To **Clear Call Blocked** for this DS1, configure this parameter to **invoke**.
5. Select **Apply**.

The online DS1s will RSIP to the default MGC. The MGC will respond with 200 OK and the gateway is ready to make calls.

Configuring Network Globals

The network globals refers to the Type Of Service (TOS) parameters. Set the Network Globals if the network the gateway is on uses TOS variables and Diffserv in its routers.

To configure Network Globals:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/Network** to display the table shown in Figure 53.

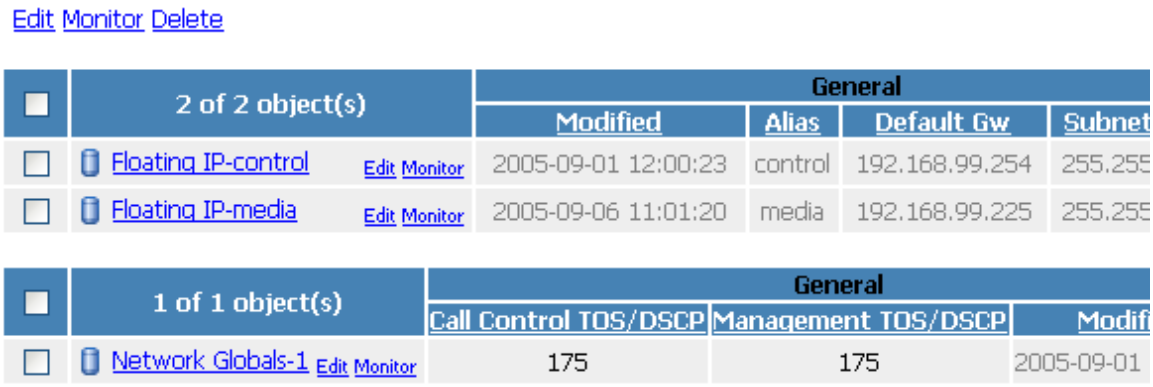


Figure 53. Network Globals Information Table

2. Click **Edit** to the right of **Network Globals-1** to display the parameters shown in Figure 54.

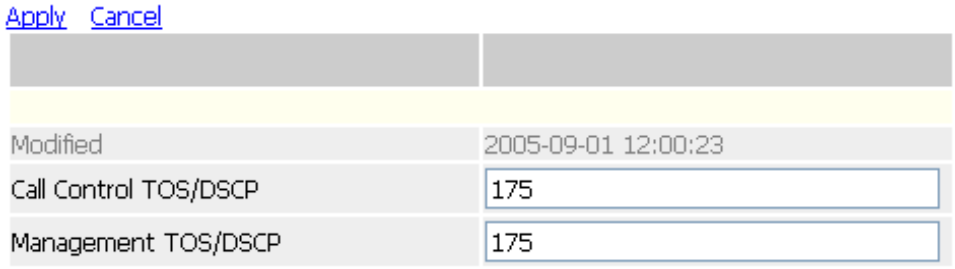


Figure 54. Network Globals Parameters

3. Configure **Call Control**. This is the value for IP TOS field for TGCP call control traffic. The default value is **112**.
4. Configure **Management**. This is the decimal value of the IP TOS field for SNMP management traffic. This value is also used for the IP TOS field of Syslog messages. The default is **112**.
5. Select **Apply**.

Configuring TrapTargets

Trap targets are used to configure the BTX-4K to send traps to specified destination IP addresses. By default, when the NE is created, the NetConductor sets one Trap target to the IP of the NetConductor. You can add up to four additional auxiliary systems to receive traps.

To add another target address:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/TrapTarget** to display the table shown in Figure 55.

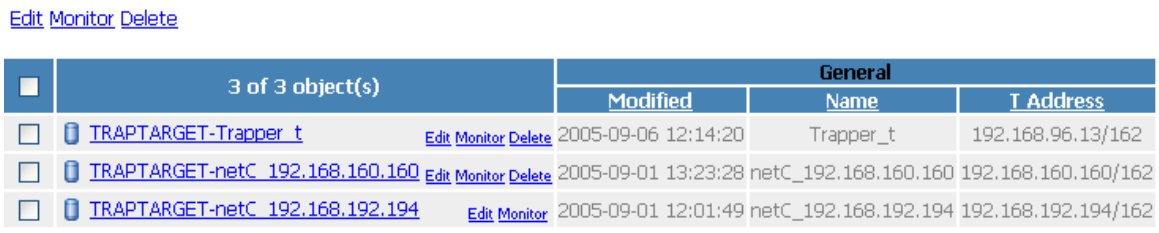


Figure 55. TrapTarget Table

2. Click **Edit** to the right of the corresponding traptarget to display the parameters shown in Figure 56.

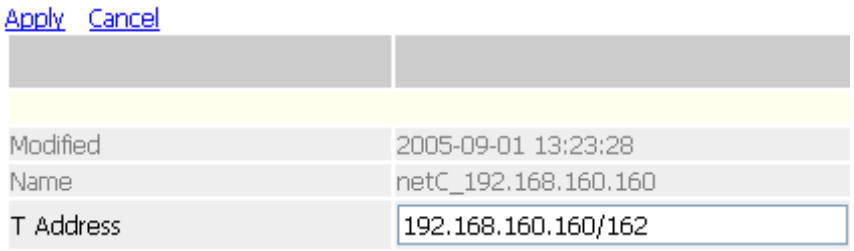
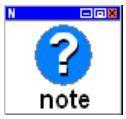


Figure 56. TrapTarget General Statistics

3. Configure **T Address**. This is the IP/UDP address of the trap target system.
4. Select **Apply**.

Configuring TFTP Clients

The BTX-4K will accept TFTP downloads from up to three (3) different clients. Downloads from clients not on this list are prohibited.



NetConductor will automatically add itself to this TFTP Client list in order to perform upgrades.

To configure the TFTP clients:

1. Expand the hierarchy in the navigation pane by selecting **Inventory** > [NE] > **Globals/TFTP** to display the TFTP Clients as shown in Figure 57.

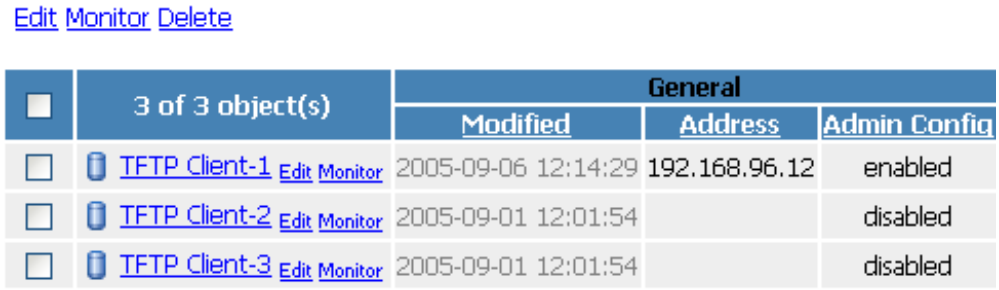


Figure 57. TFTP Client Table

2. Click **Edit** next to the TFTP client you wish to modify to display TFTP Client Settings in the Information pane, as shown in Figure 58.

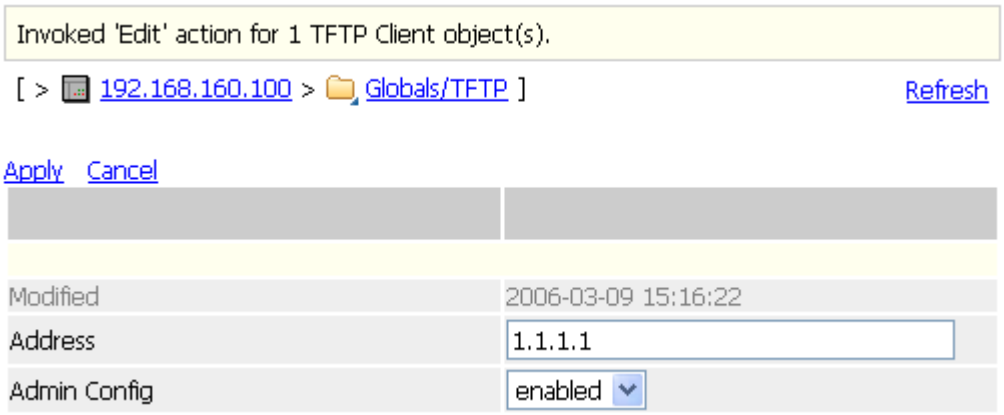


Figure 58. TFTP Client Settings

3. Configure the **Address**. This is the address of the unit that will TFTP files to the BTX-4K.
4. Enable the **Admin Config**.
5. Select **Apply**.

Configuring System Global Parameters

This section explains how to configure the parameters that apply to the entire system.

To configure the system parameters:

1. Expand the hierarchy in the navigation pane by selecting **Inventory** > [NE] > **Globals/system** to display the System Table as shown in Figure 59.

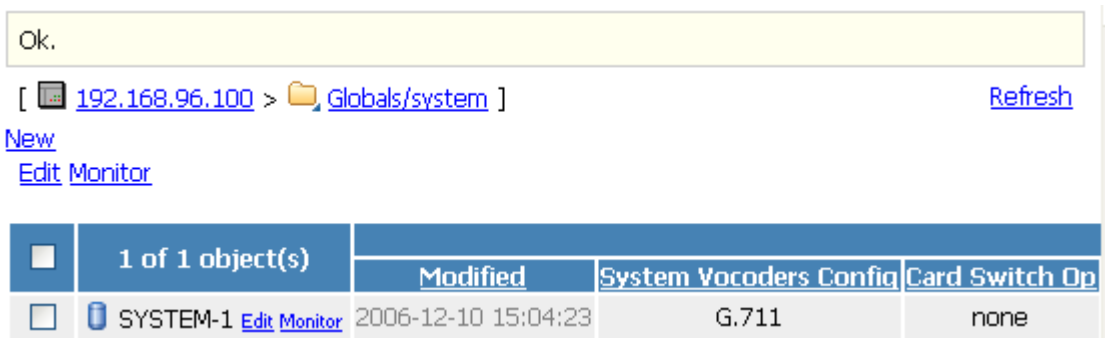


Figure 59. System Table

2. Click **Edit** next to **System-1** to display the System Settings in the Information pane, as shown in Figure 60.

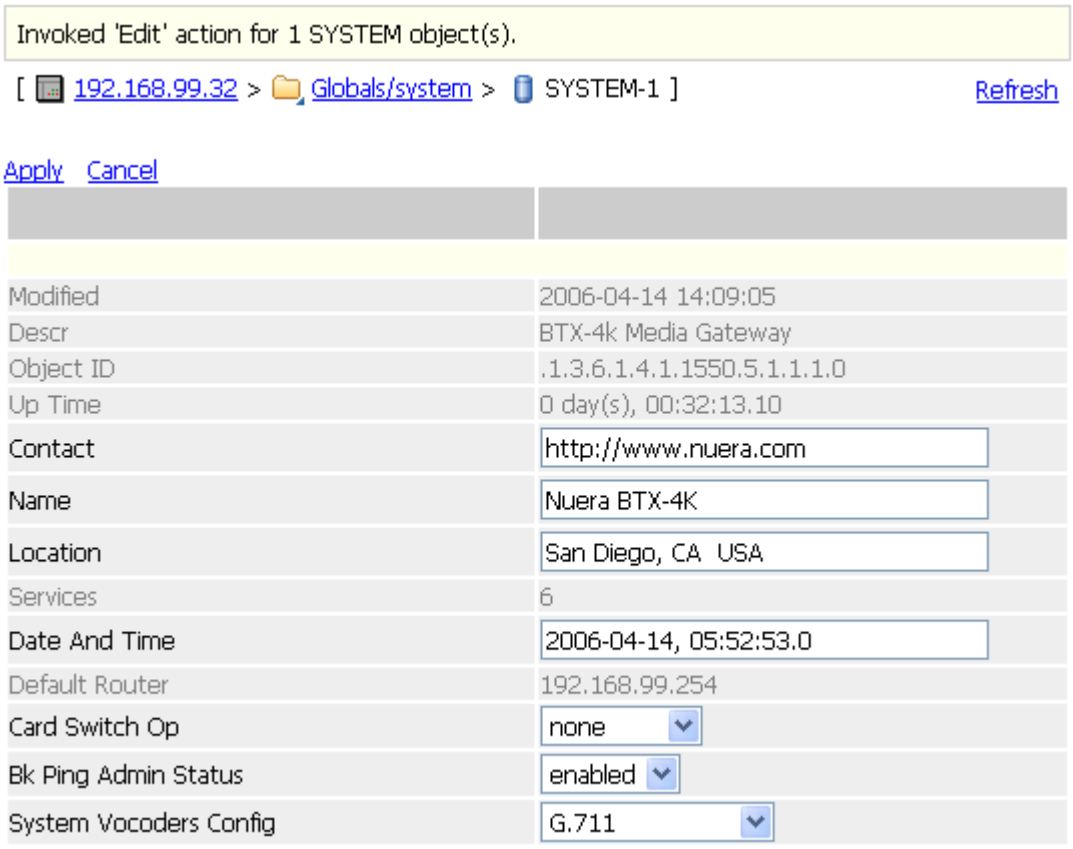


Figure 60. System Settings

3. Configure the **Contact**. This is an optional admin-defined field that displays the contact person for this managed node.
4. Configure the **Name**. This is an administratively-assigned name for this gateway.
5. Configure the **Location**. This is the physical location of this node (for example, telephone closet, 3rd floor).
6. Configure the **Date and Time**. This should be set to the current date and time. Use the format as shown: yyyy-mm-dd, hh:mm:ss.0. The gateway will use this date and time for all syslog messages it sends and logs it keeps.
7. The **Card Switch Op** allows you to perform a switch over from the active VPM card to the standby. It also performs a hardware reset of the card.
8. The **BK Ping Admin Status** allows you to **enable** or **disable** background ping monitoring. This can be useful if you have disabled ping response from your default router and want to disable VPM failures due to missed ping response. The default is **enabled**.
9. Configure **System Vocoders Config** to set the systemwide vocoder. Changing this value will change the available capacity of the system. The system must be

rebooted for this change to take effect.

If BTX-4K is not authorized for a particular vocoder, it will not show as an option.

10. Select **Apply**.

Configuring Hardware Settings

Most of the hardware configurations are preset, but there are a few that can be optionally changed. See the *ORCA-4K Hardware Manual* for more information about the hardware.

Alias and Asset ID

For every card and module in the BTX-4K, you can optionally configure an **Alias** and **Asset ID**. Setting values for these parameters can be useful for identification purposes when troubleshooting and upgrading your hardware, as shown for the Alarm Card in Figure 61. Configuring these parameters is optional and may not appear in the procedures that follow.

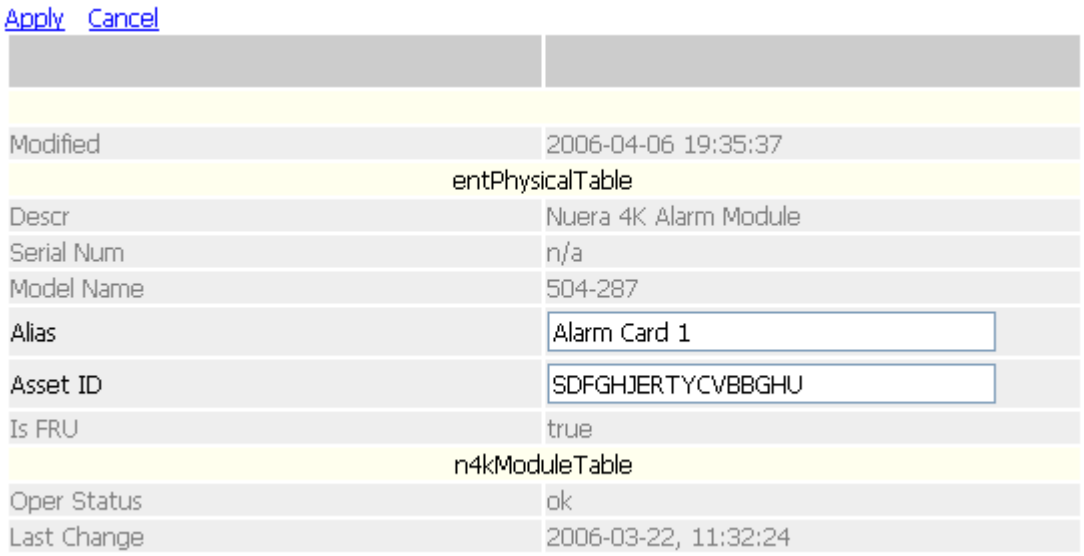


Figure 61. Alias and Asset ID - Alarm Card

Configuring a VPM Card

To configure a VPM card:

1. Expand the hierarchy by selecting **Inventory** >[NE] > **Hardware** to display the VPM table as shown in Figure 62.

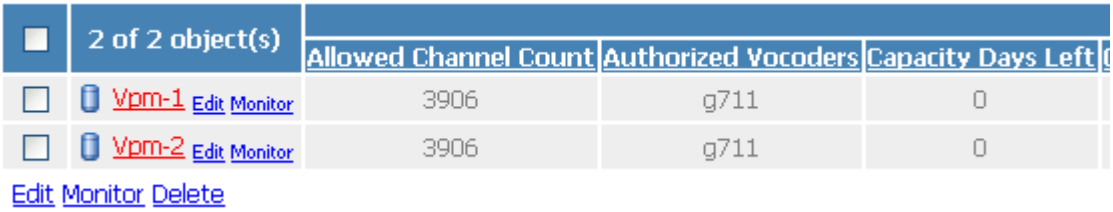


Figure 62. VPM Card Table

2. Select **Edit** next to the corresponding card to display the configurable parameters in the Information pane.

Figure 63. VPM Card Screen

3. You can perform a hardware reset of the card by selecting **reset** from the **Reset Op** drop-down menu. If you have configured a standby VPM, the system will failover to your standby card.
4. Select **OK**.

Configuring IUA

Successful IUA configuration consists of 6 steps:

1. Configure SCTP Globals
2. Configure ASP Group
3. Add ASPs
4. Add Backhaul Trunks
5. Enable ASP
6. Enable ASP Group

Configure Backhaul SCTP Globals

To configure SCTP Globals:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** > **SCTP_Globals**, as shown in Figure 64.

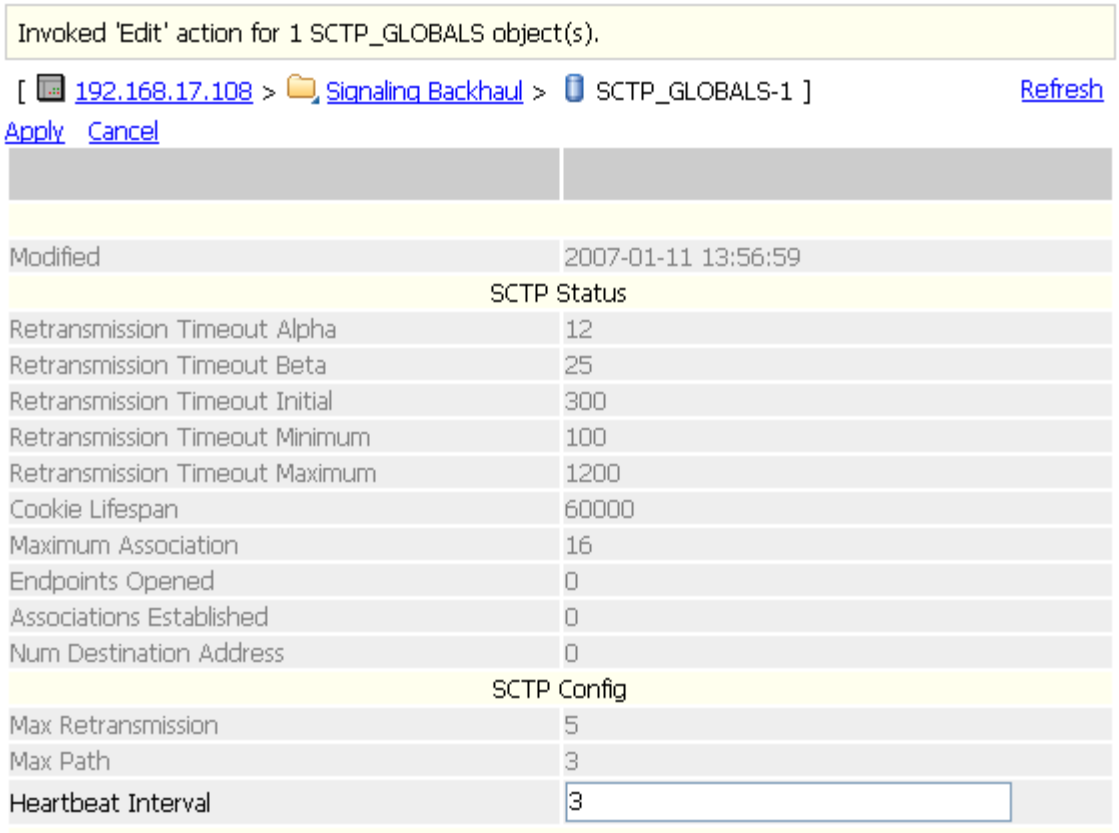


Figure 64. SCTP Global Parameters

2. Configure the **Heartbeat Interval** in seconds, from 0 to 300. Setting this value to 0 will disable the initiating heartbeat, but will still respond to incoming heartbeat with heartbeat ACK.
3. Select **Apply**. You must power-cycle your gateway before your changes will take effect.

Configure ASP Group

To configure an ASPGroup:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** as shown in Figure 65.

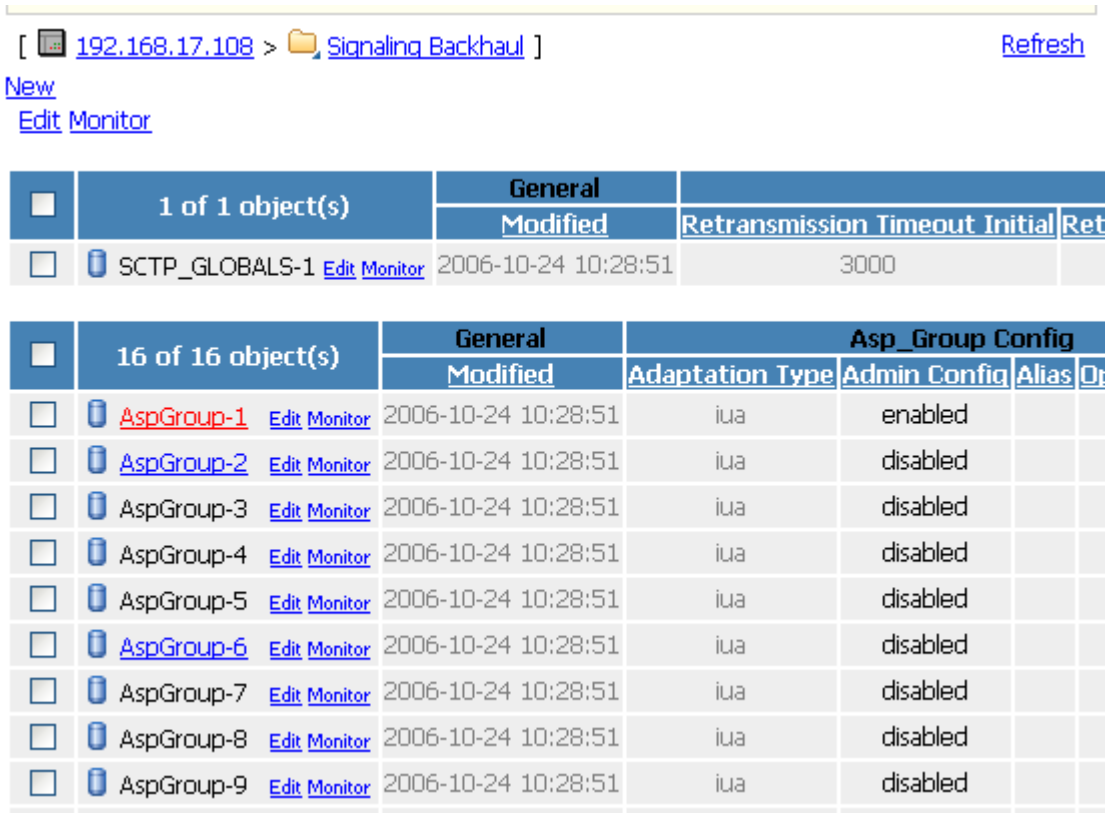


Figure 65. Signaling Backhaul Objects

2. Select **Edit** to the right of the ASPGroup to display the corresponding configuration parameters in the Information pane, as shown in Figure 66.

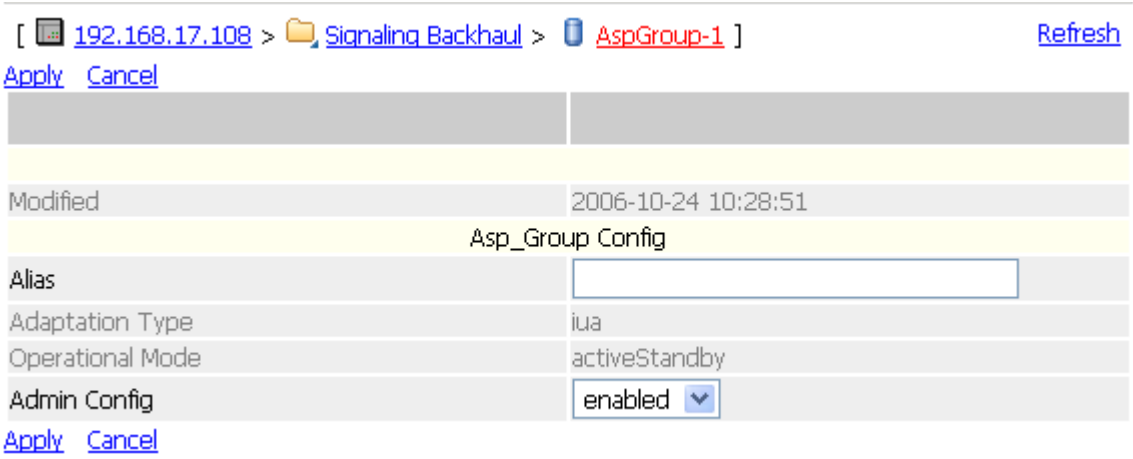


Figure 66. ASP Group Configuration Parameters

3. Enter an **Alias** to give this ASP Group a name.
4. Select **Apply** to save your changes.

DO NOT change Admin Config to "enable". This should only be done after the initial backhaul links have been added.

Add an ASP

Once you have created an ASP group, you must assign ASPs to the group. You can create up to 16 ASPs per ASP group.

To create a new ASP:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul,** as shown in Figure 67.

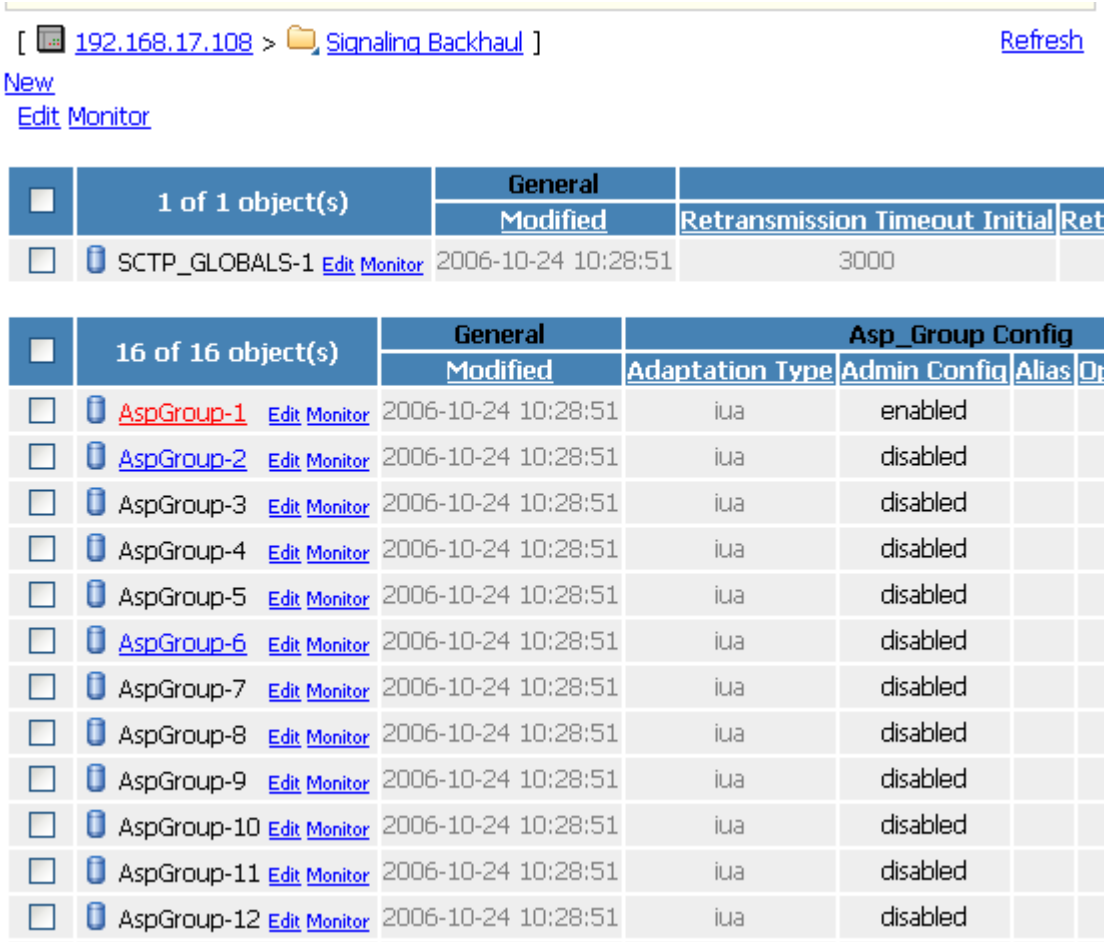

[192.168.17.108 > Signaling Backhaul]
Refresh
New
Edit Monitor
1 of 1 object(s)
General
Modified
Retransmission Timeout Initial
SCTP_GLOBALS-1 Edit Monitor
2006-10-24 10:28:51
3000
16 of 16 object(s)
General
Asp_Group Config
Modified
Adaptation Type
Admin Config
Alias
AspGroup-1 Edit Monitor 2006-10-24 10:28:51 iua enabled
AspGroup-2 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-3 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-4 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-5 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-6 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-7 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-8 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-9 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-10 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-11 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-12 Edit Monitor 2006-10-24 10:28:51 iua disabled

Figure 67. Signaling Backhaul Objects

2. Select **New** to display the Create New ASP screen, as shown in Figure 68.

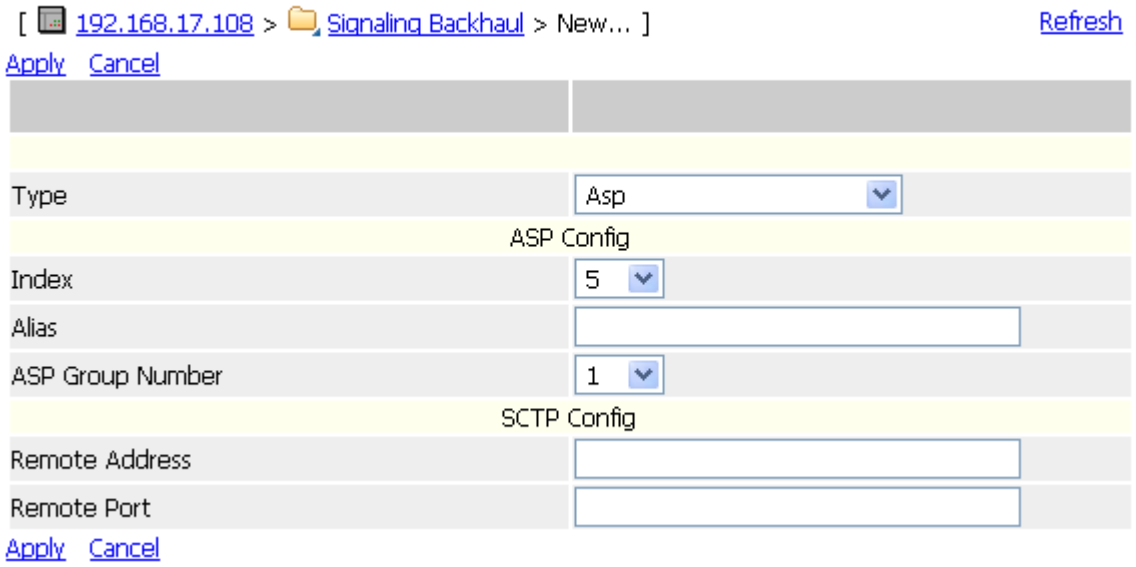


Figure 68. Create New ASP screen

3. Select **Asp** from the **Type** drop-down menu.
4. Set the **Index** value. This is the ASP number. You can define up to 16 ASPs per system.
5. Enter an **Alias** to name this ASP.
6. Select the **ASP Group Number** from 1 to 16.
7. Configure the **Remote Address** to match the IP Address of the ASP.
8. Enter the **Remote Port** to match the port used by ASP, typically 9900.
9. Select **Apply** to save your changes.

Add Backhaul Trunk

ISDN PRI trunks with a LAPD channel (FAS) should be added as backhaul trunks. ISDN trunks without LAPD (NFAS) should not be added as backhaul trunks.

To create a new Backhaul Trunk:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul,** as shown in Figure 69.

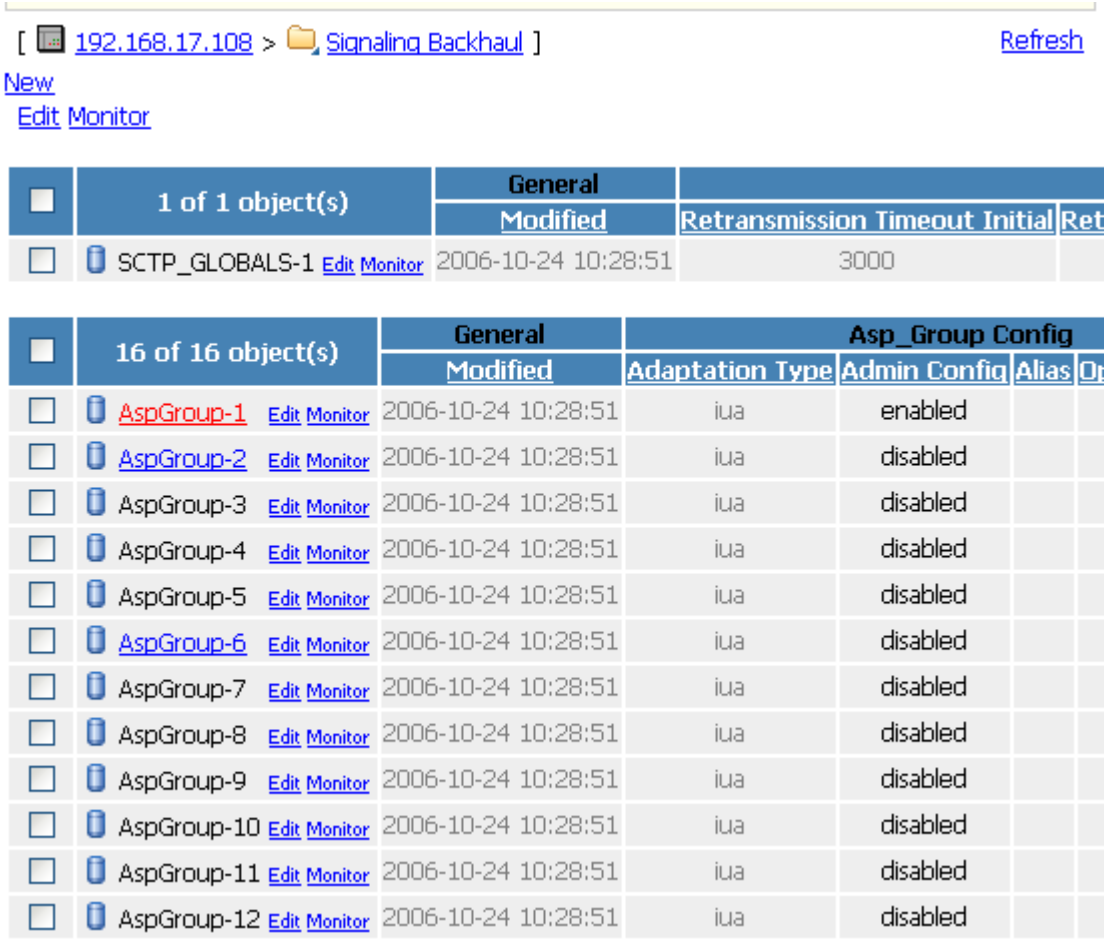

[192.168.17.108 > Signaling Backhaul]
Refresh
New
Edit Monitor
1 of 1 object(s)
General
Modified
Retransmission Timeout Initial
SCTP_GLOBALS-1 Edit Monitor
2006-10-24 10:28:51
3000
16 of 16 object(s)
General
Asp_Group Config
Modified
Adaptation Type
Admin Config
Alias
AspGroup-1 Edit Monitor 2006-10-24 10:28:51 iua enabled
AspGroup-2 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-3 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-4 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-5 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-6 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-7 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-8 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-9 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-10 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-11 Edit Monitor 2006-10-24 10:28:51 iua disabled
AspGroup-12 Edit Monitor 2006-10-24 10:28:51 iua disabled

Figure 69. Signaling Backhaul Objects

2. Select **New** to display the Create New Backhaul Trunk screen, as shown in Figure 70.

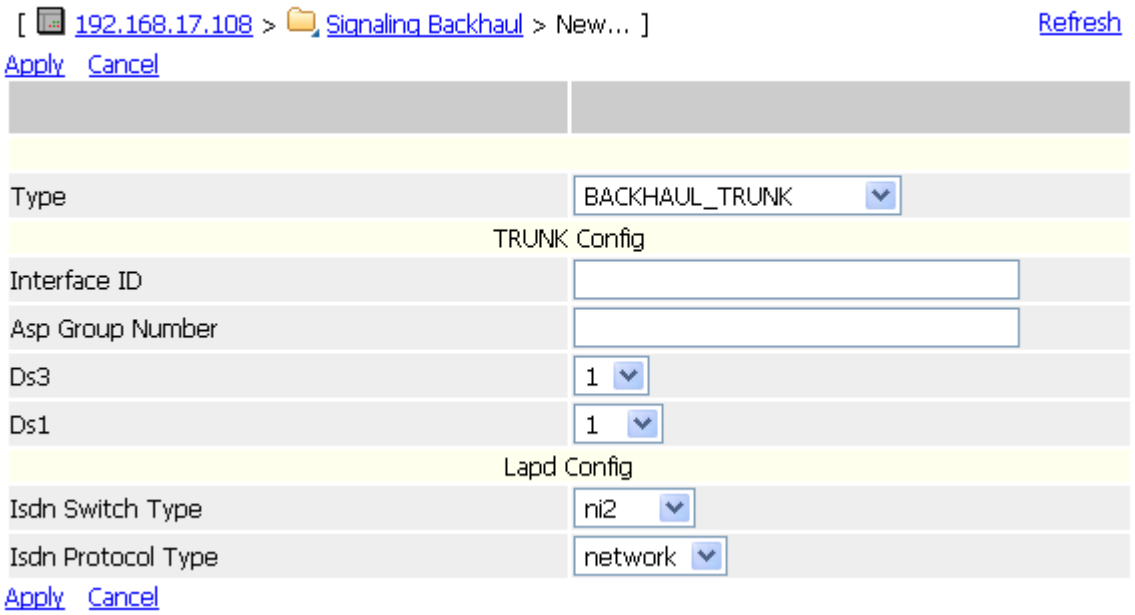
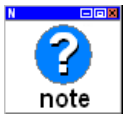


Figure 70. Create New Backhaul Trunk screen

3. Select **Backhaul_Trunk** from the **Type** drop-down menu.
4. Enter the **Interface ID**. This must be a unique integer for each system and must match the configuration in the ASP.
5. Select the **ASP Group Number** to assign the backhaul trunk to the specified ASP group. All backhaul links managed by the same ASP group must have the same ASP Group Number.
6. From the drop-down menus, select the **DS3** and **DS1** which will transport the ISDN signaling.

Verify that the Call Pro configuration of the DS1 is “isup” and the DS3 and DS1 are enabled.

7. Set the **ISDN Switch Type**. For US applications, this is usually **ni2**.
8. Configure the **ISDN Protocol Type** to match the user/network interface configuration of your gateway. The default value is **network**.
9. Select **Apply** to save your changes.



You can add Backhaul Trunks to an enabled ASP group without affecting service. Once added, properties of the Backhaul Trunks cannot be changed without deleting and readding the trunk, which IS service affecting.

Enable ASP

You can enable up to 16 ASPs per gateway.

To enable a single ASP:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** > **AspGroup-n,** as shown in Figure 71.

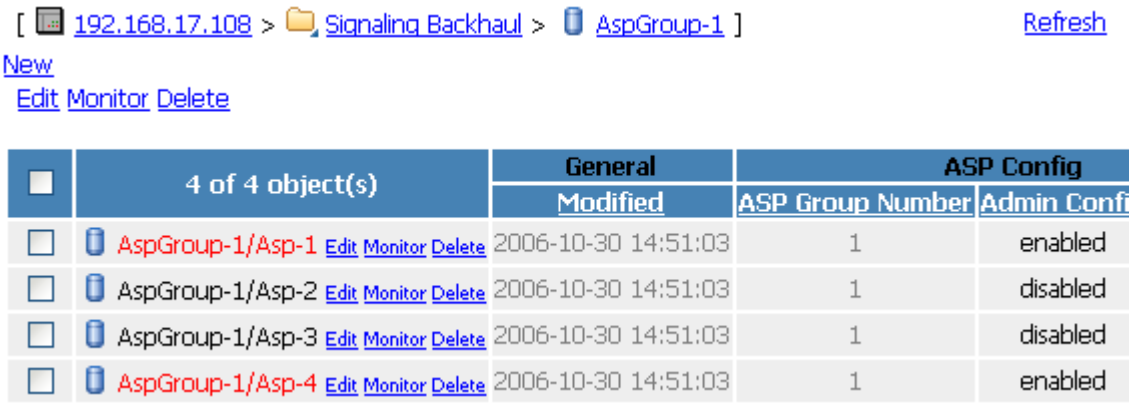


Figure 71. ASPGroup/ASP Objects

2. Select **Edit** to the right of ASP you want to enable to display ASP parameters in the information pane, as shown in Figure 72.

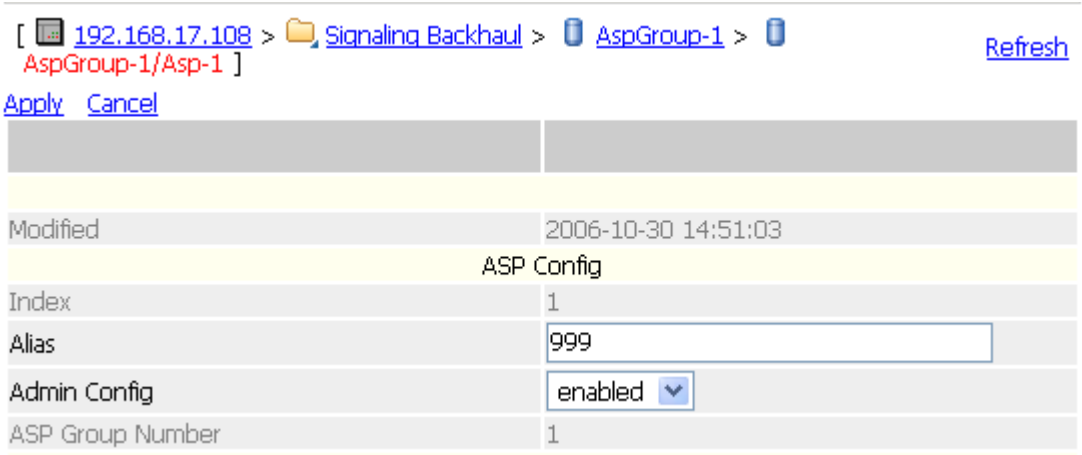


Figure 72. ASP Configuration Parameters

3. Configure the **Alias** to give this ASP an alphanumeric name.
4. From the **Admin Config** drop-down menu, select **enabled**.
5. Select **Apply** to save your changes and continue.

Verify that you have disabled the ASP Admin Config before making changes to any ASP properties, and remember to re-enable the ASP Admin Config after making changes.

Enable ASP Group

It is safe to enable the ASP Group once the initial backhaul links have been added. Additional backhaul links can be added to an enabled ASP group without affecting service.

To enable an ASP Group:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul> AspGroup-n,** as shown in Figure 73.

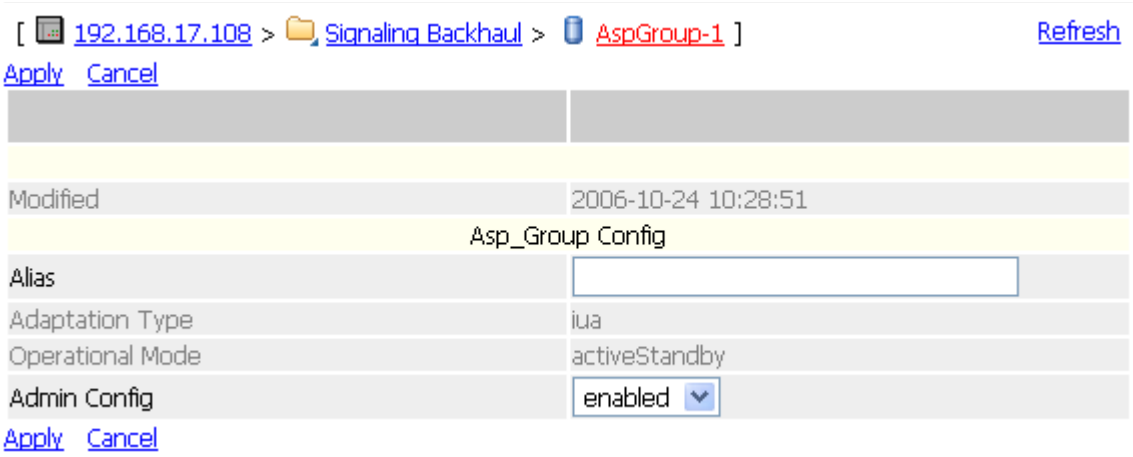


Figure 73. ASPGroup Configuration Parameters

2. Configure the **Alias** to give this ASP Group an alphanumeric name.
3. From the **Admin Config** drop-down menu, select **enabled**.
4. Select **Apply** to save your changes and continue.

4

VIEWING SYSTEM STATUS

This chapter describes the methods available for monitoring the status of your gateway. Through the hierarchy in NetConductor's Navigation pane, you can find the configurable settings and view-only statistics of your gateway.

Introduction

In NetConductor, each system entity (e.g. DS3, Ethernet interface, DNS server, etc.) contains a page of parameters you can **edit** and a **monitor** page where you can view statistics and parameter settings. By selecting a system entity in the information pane, you can display the corresponding options and statistics for that entity. Many of the screens shown in this chapter are non-configurable, view-only displays. For example, the monitor view of the Bits Interface, as shown in Figure 74, has no configurable fields.

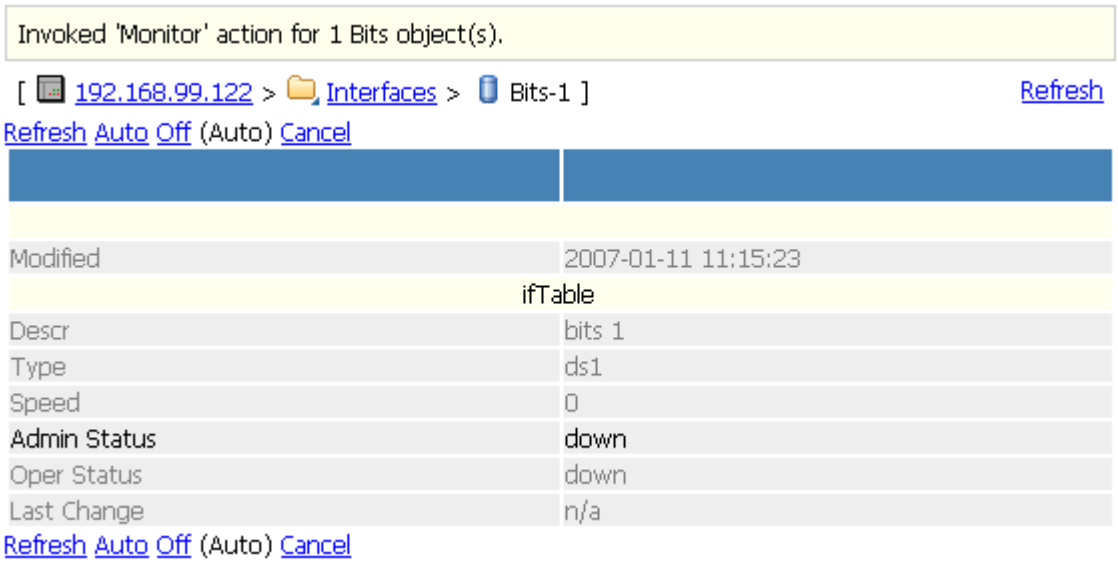
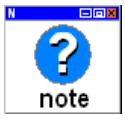


Figure 74. Floating IP Statistics



The configuration parameters detailed in this chapter are also available in the Nuera NetConductor Online Help System. Select the Help link in any NetConductor Information pane, to launch the Help System in a new browser window.

Repolling the System

As shown in Figure 75, from the **Inventory** screen in NetConductor, you can select one or more NEs and then select repoll. This will retrieve the most recent data by pulling current information from the gateway and updating the on-screen status information for the selected unit.

Figure 75. Repoll

Refresh Link

To cut down on network traffic, you can choose to **Refresh** data from the NetConductor server instead of repolling the Network Element. From any Information pane in

NetConductor, as shown in Figure 76, select **Refresh** to repopulate the screen with the most recent data from the server.

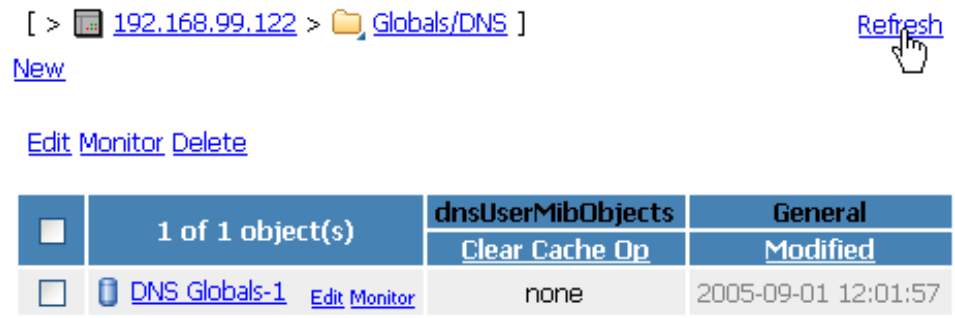


Figure 76. Refresh Link

Monitoring using NetConductor Logs

You can also utilize the logs provided by NetConductor. By selecting the **Advanced** link from the Link pane and navigating the hierarchy by selecting **Advanced** > Container > Logs the available logs will be displayed. See Figure 77. For more information on NetConductor Logs and their use, reference the NetConductor User Manual.

Figure 77. NetConductor Logs

Hardware Options and Statistics

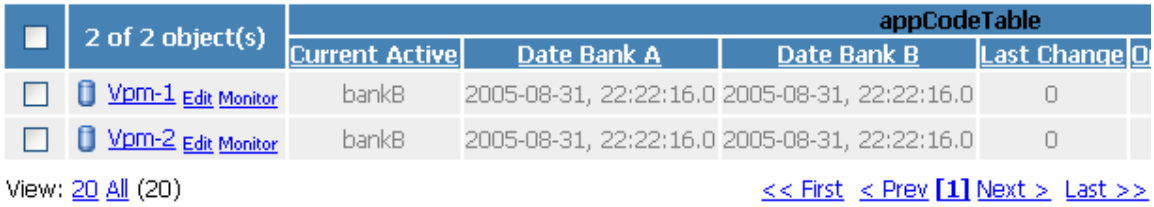
VPM Status

The following section discusses how to monitor VPM status and provides brief descriptions of each parameter or statistic.

To view VPM parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware.**
2. Select **VPM** to display the corresponding VPMs in the information pane, as

shown Figure 78.

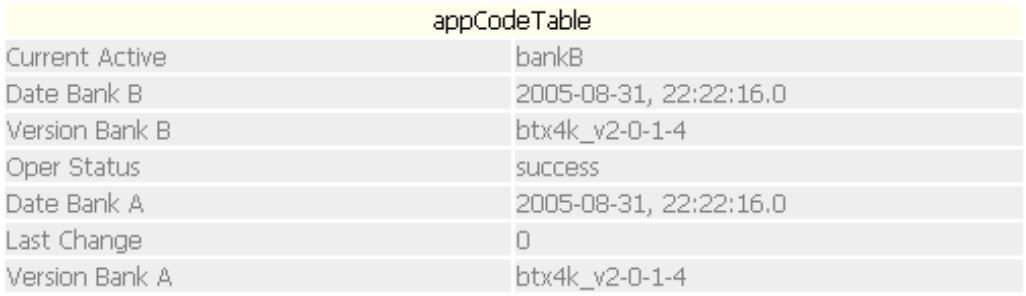


	2 of 2 object(s)	appCodeTable				
		Current Active	Date Bank A	Date Bank B	Last Change	O
☐	Vpm-1 Edit Monitor	bankB	2005-08-31, 22:22:16.0	2005-08-31, 22:22:16.0	0	
☐	Vpm-2 Edit Monitor	bankB	2005-08-31, 22:22:16.0	2005-08-31, 22:22:16.0	0	

View: 20 All (20) << First < Prev [1] Next > Last >>

Figure 78. VPM Information pane

3. Select the **Monitor** link to the right of the appropriate VPM. The table displayed has been broken up in the following figures and sections (shown in order) to improve readability.



appCodeTable	
Current Active	bankB
Date Bank B	2005-08-31, 22:22:16.0
Version Bank B	btx4k_v2-0-1-4
Oper Status	success
Date Bank A	2005-08-31, 22:22:16.0
Last Change	0
Version Bank A	btx4k_v2-0-1-4

Figure 79. VPM General Statistics

Current Active

The bank (A or B) from which the current, active code was retrieved at powerup or reset.

Date Bank B

The version date of the code in Bank B.

Version Bank B

The version number of the code in Bank B.

Oper Status

The operational status of the most recent code upgrade. This will show success if a reset or power-cycle has occurred since the code upgrade.

Date Bank A

The version date of the code in Bank A.

Last Change

The time when the most recent code upgrade occurred. Note that a card reset will also change this time.

Version Bank A

The version number of the code in Bank A.

entPhysicalTable	
Descr	Nuera 4K Motherboard
Hardware Rev	25
Software Rev	see appCodeTable
Serial Num	120510805
Model Name	555
Alias	
Asset ID	
Is FRU	true

Figure 80. VPM entPhysicalTable Statistics

Descr

Nuera's name for the card or module.

Hardware Rev

The current hardware revision for the card or module.

Software Rev

The current software revision for the entity, if applicable.

Serial Num

The serial number for the card or module.

Model Name

The Nuera part number.

Alias

A user-defined label for the card or component.

Asset ID

A user-defined ID label for the card or component.

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

n4kAuthorizationTable	
Maximum Channel Count	1344
Allowed Channel Count	1344
Authorized Vocoders	g711
Vocoders Oper Status	g711
Capacity Upgrade Oper Status	success
Capacity Upgrade Oper Status Last Change	2006-02-21, 18:01:01
Vocoders Upgrade Oper Status	success
Vocoders Upgrade Oper Status Last Change	2006-02-21, 17:32:57
Capacity License Type	permanent
Vocoders License Type	permanent
Capacity Days Left	0
Vocoders Days Left	0
Pending Channel Count	3360
Pending Vocoders	

Figure 81. VPM n4kAuthorizationTable Statistics

Maximum Channel Count

This returns the maximum number of channels that can run calls on this VPM based on the authorization. The actual (allowed) number of channels may be lower than this value when different vocoders are chosen.

Allowed Channel Count

The number of channels available for use with the chosen vocoder(s).

Authorized Vocoders

This shows the vocoders based on the authorization.

Vocoders Oper Status

This displays the vocoder suite currently running on the VPM.

Capacity Upgrade Oper Status

The operational state of the most recent authorization update for capacity.

Capacity Upgrade Oper Status Last Change

The time when the authorization capacity upgrade operational status last changed. Note that a power cycle will also change this value.

Vocoders Upgrade Oper Status

The operational state of the most recent authorization update for vocoder.

Vocoders Upgrade Oper Status Last Change

The time when the authorization vocoder upgrade operational status last changed. Note that a power cycle will also change this value.

Capacity License Type

The capacity authorization type can be temporary or permanent. A permanent authorization does not expire. When the temporary authorization expires, the VPM will restart and will not be able to run any calls. You should contact TAC to obtain a new key.

Vocoders License Type

The vocoder authorization type can be temporary or permanent. A permanent authorization does not expire. When the temporary authorization expires, the VPM will restart and will not be able to run any calls. You should contact TAC to obtain a new key.

Capacity Days Left

The number of days left for the authorized capacity. If the authorization is permanent, its value is 0 and can be discarded. If the authorization is temporary, a value of 0 means the key has expired and the VPM can no longer run any calls.

Vocoders Days Left

Number of days left for the authorized vocoders. If the authorization is permanent, its value is 0 and can be discarded. If the authorization is temporary, a value of 0 means the key has expired and the VPM can no longer run any calls.

Pending Channel Count

This value displays the pending capacity authorization on this VPM. When this value is non-zero, then a reset of this VPM is required to activate the new capacity authorization.

Pending Vocoders

This value displays the pending vocoder authorization on this VPM. When this value is non-zero, then a reset of this VPM is required to activate the new vocoder authorization.

n4kCardStatsTable	
Buffer Avail	30444
Idle Time	97
Partition Avail	6047
Heap Avail	3810224

Figure 82. VPM n4kCardStatsTable Statistics

Buffer Avail

The number of available buffers.

Idle Time

The CPU idle time of the current card, measured in %, over a period of 4 seconds.

Partition Avail

The number of available partitions.

Heap Avail

The number of heap bytes available.

n4kCardTable	
Oper Status	active
Last Change	2006-09-04, 13:13:25
Reset Op	none

Figure 83. VPM n4kCardTable Statistics

Last Change

The time of when the VPM operational status last changed.

Reset Op

Performs a hardware reset of the card. Note that, if applicable, a fail over will be attempted.

Oper Status

The current operational state of the card.

n4kPwrTable	
Oper Status	ok
Last Change	2005-09-06, 11:44:45

Figure 84. VPM n4kPwrTable Statistics

Oper Status (Power)

The current operational status of the power rails & associated fuses.

Last Change (Power)

The time when the power operational status last changed.

BCM Status

The following section shows you how to monitor BCM status and provides brief descriptions of each parameter or statistic.

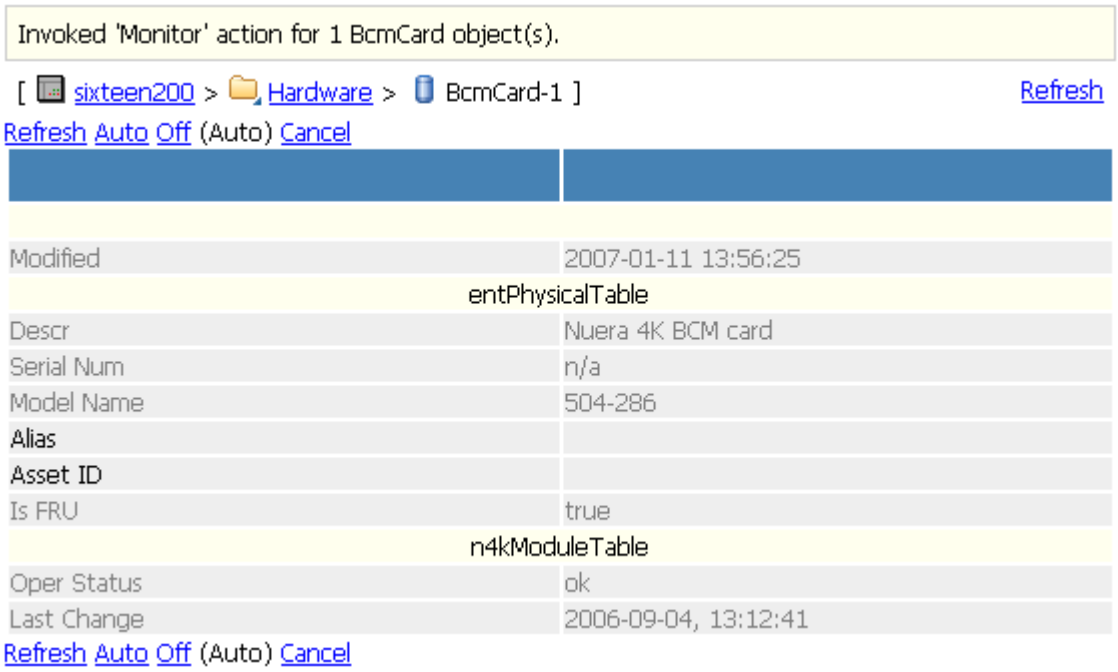
To view BCM parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware.**
2. Select **BCM** to display the list of corresponding BCMs in the information pane, as shown Figure 85.

	2 of 2 object(s)	entPhysicalTable				
		Alias	Asset ID	Descr	Firmware Rev	Hardware
☐	BcmCard-1 Edit Monitor			Nuera 4K BCM card		
☐	BcmCard-2 Edit Monitor			Nuera 4K BCM card		

Figure 85. Hardware Table (BCM portion shown)

3. Select the **Monitor** link to the right of the appropriate BCM. The table shown in Figure 86 is displayed.



Invoked 'Monitor' action for 1 BcmCard object(s).

[sixteen200 > Hardware > BcmCard-1] Refresh

Refresh Auto Off (Auto) Cancel

Modified	2007-01-11 13:56:25
entPhysicalTable	
Descr	Nuera 4K BCM card
Serial Num	n/a
Model Name	504-286
Alias	
Asset ID	
Is FRU	true
n4kModuleTable	
Oper Status	ok
Last Change	2006-09-04, 13:12:41

Refresh Auto Off (Auto) Cancel

Figure 86. BCM General and Module Specific Statistics

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the card or component.

Alias

A user-defined label for the card or component.

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module. Non-viewable.

Last Change

The timestamp marking the last change to Oper Status.

Oper Status

The current operational status of the card or module.

OCMCard Status

The following section shows you how to monitor OCMCard status and provides brief descriptions of each parameter of statistic.

To view OCM Card parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware** to display the corresponding OCM Cards in the information pane, as shown Figure 87.

	2 of 2 object(s)	entPhysicalTable				
		Alias	Asset ID	Descr	Is FRU	Mode
☐	OCMCard-1 Edit Monitor	OCM Card	123456	Nuera 4K OCM card	true	50
☐	OCMCard-2 Edit Monitor	fswrsfwtsdgwerfaw	farfarzsdarqaf	Nuera 4K OCM card	true	50

Figure 87. Hardware Table (OCMCard portion shown)

2. Select **Monitor** to the right of the appropriate OCMCard to display the table shown in Figure 88.

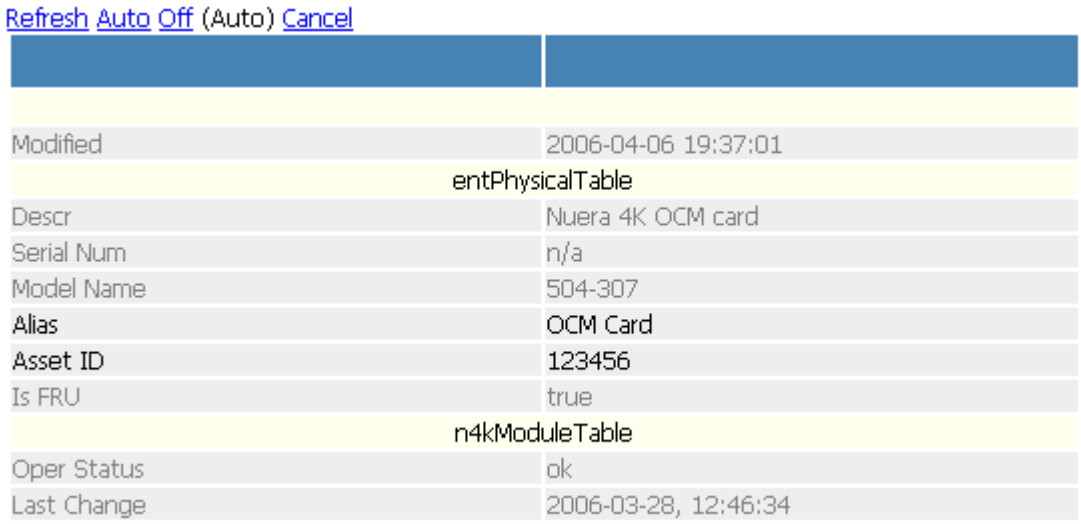


Figure 88. OCM Card General and Module Specific Statistics

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module.

Model Name

The Nuera part number.

Alias

A user-defined label for the card or component.

Asset ID

A user-defined ID label for the card or component.

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Oper Status

The current operational status of the card or module.

Last Change

The timestamp marking the last change to Oper Status.

OC3DB Card Status

The following section discusses how to monitor OC3DB status and provides brief descriptions of each parameter or statistic.

To view OC3DB parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware** > **Vpm-n.**
2. Select **Vpm-n/OC3db** to display the corresponding OC3DB near the bottom of the information pane, as shown Figure 89.

	1 of 1 object(s)	entPhysicalTable			
		Alias	Asset ID	Descr	Is F
☐	Vpm-1/OCMdb-18 Edit Monitor	OC3Module	OC3Module	Nuera 4K OC3 Interface Module	fals

Figure 89. Hardware Table (OC3DB portion shown)

3. Select the **Monitor** link to the right of the appropriate OC3DB. The table shown in Figure 90 is displayed.

Modified	2006-09-24 17:59:12
entPhysicalTable	
Descr	Nuera 4K OC3 Interface Module
Serial Num	370507394
Model Name	504-305
Alias	
Asset ID	
Is FRU	false
Hardware Rev	8
n4kModuleTable	
Oper Status	ok
Last Change	2000-03-18, 16:40:07

Refresh Auto Off (Auto) Cancel

Figure 90. OC3DB General and Module Specific Statistics

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module.

Model Name

The Nuera part number.

Alias

A user-defined label for the card or component.

Asset ID

A user-defined ID label for the card or component.

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Hardware Rev

The hardware revision number of the card or module.

Oper Status

The current operational status of the card or module.

Last Change

The timestamp marking the last change to Oper Status.

DS3DB Card Status

The following section discusses how to monitor DS3DB status and provides brief descriptions of each parameter or statistic.

To view DS3DB parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware** > **Vpm-n.**
2. Select **Vpm-n / DS3DB** to display the corresponding DS3DBs in the information pane, as shown Figure 91.

Figure 91. Hardware Table (DS3DB portion shown)

3. Select the **Monitor** link to the right of the appropriate DS3DB. The table shown in Figure 92 is displayed.

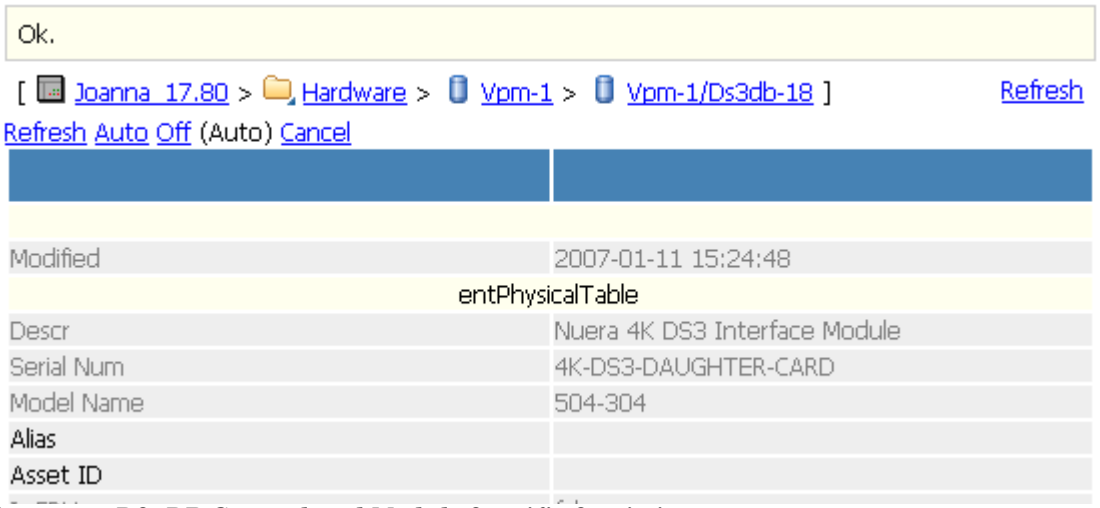


Figure 92. DS3DB General and Module Specific Statistics

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the card or component.

Hardware Rev

The hardware revision number of the card or module.

Alias

A user-defined label for the card or component.

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module.

Oper Status

The current operational status of the card or module.

Last Change

The timestamp marking the last change to Oper Status.

DSP Status

The following section discusses how to monitor DSP status and provides brief descriptions of each parameter or statistic.

To view DSP parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware > Vpm-n**.
2. Select **DSP** to display the corresponding DSP Module in the information pane, as shown Figure 93.

	16 of 16 object(s)	Current Active	Date Bank A	Date Bank
☐	Vpm-1/Dsp-1 Edit Monitor	bankB	2005-08-31, 22:49:07.0	2005-08-31, 22:
☐	Vpm-1/Dsp-2 Edit Monitor	bankB	2005-08-31, 22:49:07.0	2005-08-31, 22:
☐	Vpm-1/Dsp-3 Edit Monitor	bankB	2005-08-31, 22:49:07.0	2005-08-31, 22:
☐	Vpm-1/Dsp-4 Edit Monitor	bankB	2005-08-31, 22:49:07.0	2005-08-31, 22:
☐	Vpm-1/Dsp-5 Edit Monitor	bankB	2005-08-31, 22:49:07.0	2005-08-31, 22:

Figure 93. Hardware Table (Vpm portion shown)

3. Select the **Monitor** link to the right of the appropriate DSP. The table shown in Figure 94 is displayed.

appCodeTable	
Date Bank A	2005-08-31, 22:49:07.0
Current Active	bankB
Date Bank B	2005-08-31, 22:49:07.0
Last Change	0
Version Bank B	btx4k_v2-0-1-4
Version Bank A	btx4k_v2-0-1-4
Oper Status	success
entPhysicalTable	
Is FRU	true
Model Name	504-302
Firmware Rev	
Descr	Nuera 4K DSP Module
Serial Num	n/a
Asset ID	
Hardware Rev	*
Alias	
n4kModuleTable	
Oper Status	ok
Last Change	2005-09-06, 11:44:45

Figure 94. DSP General, Codes and Module Statistics

Date Bank A

The version date of the code in Bank A.

Current Active

Displays the bank (A or B) from which the current, active code was retrieved at powerup or reset. This value is the same for all DSP entities.

Date Bank B

The version date of the code in Bank B.

Last Change

The time when the most recent code upgrade occurred. Note that a card reset will also change this time.

Version Bank B

The version number of the code in Bank B.

Version Bank A

The version number of the code in Bank A.

Oper Status

The operational state of the most recent code update.

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Firmware Rev

Not currently used.

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module.

Asset ID

A user-defined ID label for the card or component.

Hardware Rev

The hardware revision number of the card or module.

Alias

A user-defined label for the card or component.

Oper Status (Module Specific)

The current operational status of the card or module.

Last Change (Module Specific)

The timestamp marking the last change to Oper Status for the module.

NP Status

The following section discusses how to monitor NP status and provides brief descriptions of each parameter or statistic.

To view Network Processor (NP) parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware > NP-nn**.
2. Select **NP** to display the corresponding Network Processor module in the information pane, as shown Figure 95.

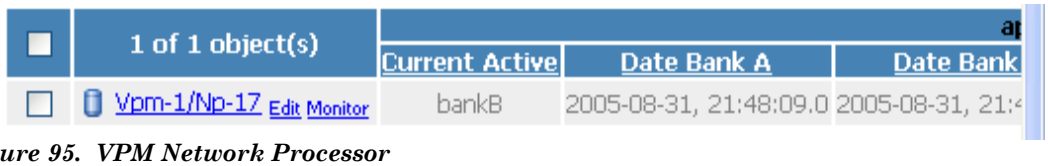


Figure 95. VPM Network Processor

3. Select the **Monitor** link to the right of the appropriate NP. The table shown in Figure 96 is displayed.

appCodeTable	
Date Bank A	2005-08-31, 21:48:09.0
Current Active	bankB
Date Bank B	2005-08-31, 21:48:09.0
Last Change	0
Version Bank B	btx4k_v2-0-1-4
Version Bank A	btx4k_v2-0-1-4
Oper Status	success
entPhysicalTable	
Is FRU	false
Model Name	504-303
Firmware Rev	
Descr	Nuera 4K NP Module
Serial Num	300410719
Asset ID	
Hardware Rev	8
Alias	
n4kModuleTable	
Oper Status	ok
Last Change	2005-09-06, 11:44:45

Figure 96. NP General, Codes and Module Specific Statistics

Date Bank A

The version date of the code in Bank A.

Current Active

Displays the bank (A or B) from which the current, active code was retrieved at powerup or reset.

Date Bank B

The version date of the code in Bank B.

Last Change

The time when the most recent code upgrade occurred. Note that a card reset will also change this time.

Version Bank B

The version number of the code in Bank B.

Version Bank A

The version number of the code in Bank A.

Oper Status (Module Specific)

The current operational status of the card or module.

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Firmware Rev

Not currently used.

Descr

Nuera's name for the NP.

Serial Num

The serial number for the NP.

Asset ID

A user-defined ID label for the NP.

Hardware Rev

The hardware revision number of the NP.

Alias

A user-defined label for the NP.

Oper Status

The operational state of the most recent code update.

Last Change (Module Specific)

The time when the most recent code upgrade occurred. Note that a card reset will also change this time.

Fan Status

The following section discusses how to monitor Fan status and provides brief descriptions of each parameter or statistic.

To view Fan options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware**.
2. Select the **FANTray** link to display the corresponding information, as shown Figure 97.

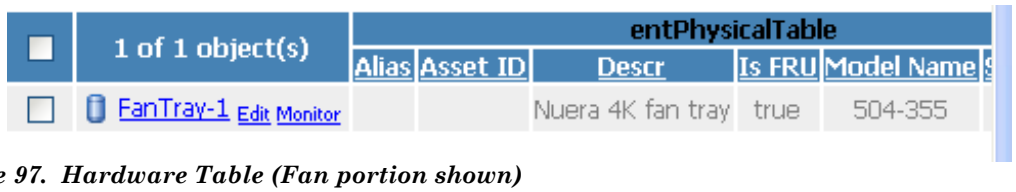


Figure 97. Hardware Table (Fan portion shown)

3. Select the **Monitor** link to the right of the **FANTray** link to display the corresponding information, as shown Figure 97.

Is FRU	true
Model Name	504-355
Asset ID	
Alias	
Descr	Nuera 4K fan tray
Serial Num	n/a
n4kFanStatus	
Oper Status	ok
Last Change	2005-09-06, 11:44:45

Figure 98. Fan General and Fan Specific Statistics

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the fan.

Alias

A user-defined label for the fan.

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the fan. Non-viewable.

Oper Status

The current operational status of the fan.

Last Change

The timestamp marking the last change to Oper Status.

DS3X Status

The following section discusses how to monitor DS3X status and provides brief descriptions of each parameter or statistic.

To view DS3X options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware**. The table shown in Figure 99 will appear.

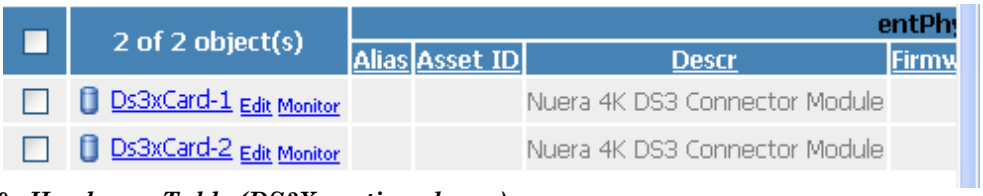


Figure 99. Hardware Table (DS3X portion shown)

2. Select the **Monitor** link to the right of the **Ds3xCard-n** link to display the corresponding information, as shown Figure 100.

Modified	2006-09-21 12:58:07
entPhysicalTable	
Descr	Nuera 4K DS3 Connector Module
Serial Num	n/a
Model Name	504-288
Alias	
Asset ID	
Is FRU	true
n4kModuleTable	
Oper Status	ok
Last Change	2006-08-18, 07:07:14

Figure 100. DS3X General and Module Specific Statistics

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the card or component.

Alias

A user-defined label for the card or component.

Descr

Nuera's name for the card or module.

Serial Num

The serial number for the card or module. Non-viewable.

Oper Status

The current operational status of the card or module.

Last Change

The timestamp marking the last change to Oper Status.

Sensor Status

The following section discusses how to monitor Sensor status and provides brief descriptions of each parameter or statistic.

To view Sensor options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Hardware** > **VPM-n**. The table shown in Figure 101 will appear.

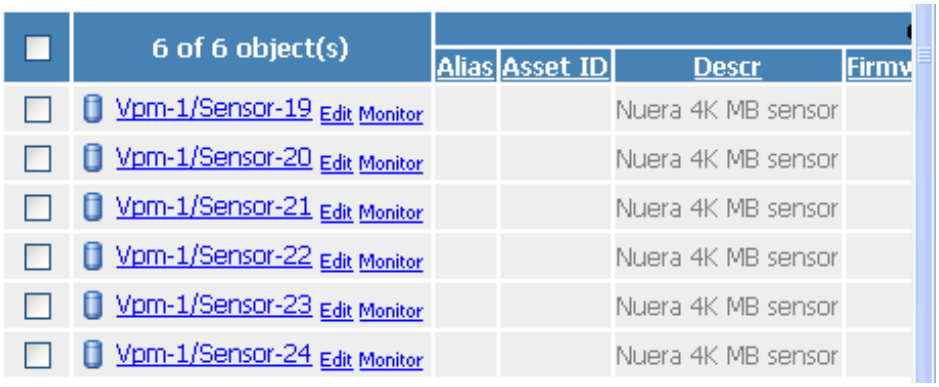


Figure 101. Hardware Table (Sensor portion shown)

2. Select the **Monitor** link to the right of the **Vpm-1/Sensor-nn** link to display the corresponding information, as shown Figure 102.

Is FRU	false
Model Name	MB sensor
Asset ID	
Hardware Rev	
Alias	
Firmware Rev	
Descr	Nuera 4K MB sensor
Serial Num	n/a
n4kSensTable	
Last Change	2005-09-06, 11:44:45
Current Temp	27
Oper Status	ok

Figure 102. Sensor Statistics

Is FRU

This flag indicates whether or not this module is considered a "field replaceable unit".

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the Sensor.

Alias

A user-defined label for the Sensor.

Descr

Nuera's name for the Sensor.

Last Change (Sensor Specific)

The timestamp marking the last change to Oper Status.

Current Temp

The current temperature as reported by the temperature sensor (in celsius).

Oper Status (Sensor Specific)

The current operational status of the card or module.

ALARM Status

The following section discusses how to monitor Alarm status and provides brief descriptions of each parameter or statistic.

To view ALARM options and statistics:

1. Expand the hierarchy by selecting **Inventory** > **Network** > [NE] > **Hardware**. The table shown in Figure 103 will appear in the Information pane.

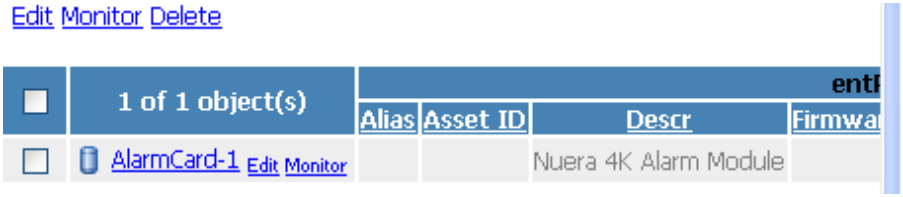


Figure 103. Hardware Table (Alarm portion shown)

2. Select the **Monitor** link to the right of the **AlarmCard-1** link to display the corresponding information, as shown Figure 104.

Modified	2006-09-21 12:56:17
entPhysicalTable	
Descr	Nuera 4K Alarm Module
Serial Num	n/a
Model Name	504-287
Alias	
Asset ID	
Is FRU	true
n4kModuleTable	
Oper Status	ok
Last Change	2006-08-18, 07:07:14

Figure 104. ALARM General and Module Specific Statistics

Is FRU

This flag indicates whether or not this module is considered a “field replaceable unit”.

Model Name

The Nuera part number.

Asset ID

A user-defined ID label for the Alarm module.

Alias

A user-defined label for the Alarm module.

Descr

Nuera's name for the Alarm module.

Serial Num

The serial number for the Alarm module. Non-viewable.

Last Change (Alarm Specific)

The timestamp marking the last change to Oper Status.

Oper Status (Alarm Specific)

The current operational status of the Alarm module.

Interface Parameters and Statistics

Ethernet Status

The following section discusses how to monitor Ethernet status and provides brief descriptions of each parameter or statistic.

To view Ethernet options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces**. The table shown in Figure 105 will appear.

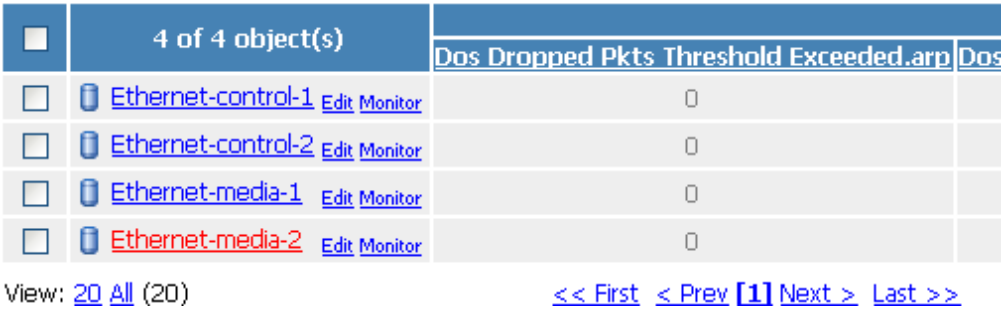


Figure 105. Interface Table (Ethernet shown)

2. Select the **Monitor** link to the right of the **Ethernet-control-n/media-n** link to display the corresponding information. The table displayed has been broken up in the following figures and sections (shown in order) to improve readability.

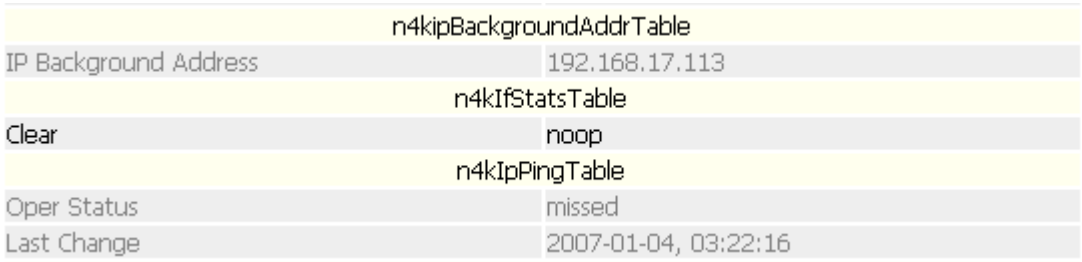


Figure 106. IP Background Address Table

IP Background Address

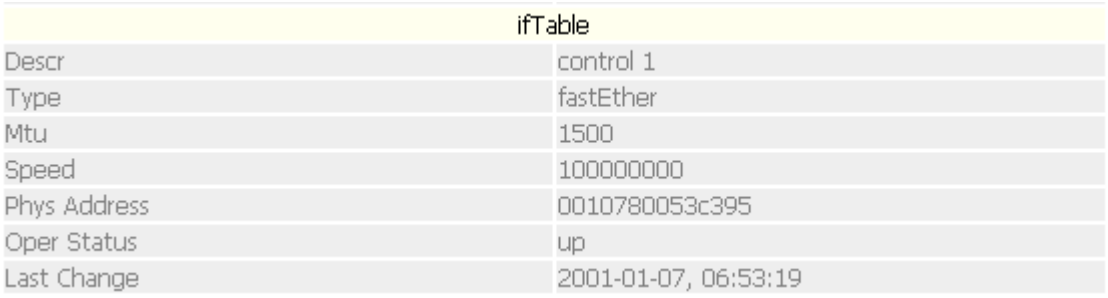
The background IP address assigned to this physical interface.

Oper Status

The operational status of the heartbeat ping to default router for this Ethernet interface.

Last Change

The time and date of the last change to the operational status of this interface.



ifTable	
Descr	control 1
Type	fastEther
Mtu	1500
Speed	100000000
Phys Address	0010780053c395
Oper Status	up
Last Change	2001-01-07, 06:53:19

Figure 107. Ethernet ifTable

Descr

Nuera's name for the interface.

Type

The type of interface.

MTU

The size of the largest packet which can be sent or received on the interface, specified in octets.

Speed

The maximum bandwidth in bits per second.

Physical Address

The MAC address of the interface.

Oper Status

The current operational status of the interface.

Last Change

The timestamp marking the last change to Oper Status.

DoS Statistics

The partial DoS Statistics table shown in Figure 108, allows you to view statistics regarding Denial of Service (DoS).

DoS Statistics	
Ingress Table Lookup Failures.kerberosback	0
Ingress Table Lookup Failures.mobile	0
Ingress Table Lookup Failures.enetunknown	0
Ingress Table Lookup Failures.enetbroadcastunknown	0
Ingress Table Lookup Failures.xgcp	0
Ingress Table Lookup Failures.tftp	0
Ingress Table Lookup Failures.snmp	0
Ingress Table Lookup Failures.sctp	0
Ingress Table Lookup Failures.icmpfloat	0
Ingress Table Lookup Failures.enetmulticastunknown	0
Ingress Table Lookup Failures.icmpback	0
Ingress Table Lookup Failures.udpunknown	0
Ingress Table Lookup Failures.arp	0
Ingress Table Lookup Failures.other	0
Ingress Table Lookup Failures.mirror	0
Ingress Table Lookup Failures.ikefloat	0
Ingress Table Lookup Failures.ipunknown	0

Figure 108. Ethernet DoS Statistics

DoS Traffic Flow Types

A traffic flow is a particular Ethernet or IP packet type. Some flow types are allowed on certain ports (media vs. control) and some flow types are not allowed into the BTX-4K at all. There are four types of DoS Traffic Flow:

- **Ingress Table Lookup Failures** - This is a count of the number of incoming packets for the particular packet flow that are dropped because those packets are not allowed into the particular Ethernet port at all.
- **DoS Dropped Pkts Threshold Exceeded** - This is a count of the number of incoming packets for the particular packet flow that are dropped because the denial of service threshold has been crossed for the particular flow on the particular Ethernet port. Packets of that flow type are dropped until the denial of service rate has dropped below the threshold.
- **DoS Threshold Crossed** - This is a status that indicates whether a particular flow has crossed the denial of service threshold. A flow type with an exceeded status will be dropping packets of that same flow type until the status drops back to nonExceeded.

- **DoS Threshold Crossed Last Change** - This is the time when the DoS Threshold Crossed changed state, either going to the exceeded state or going back to the notExceeded state.

Flow Types

Flow types are listed in Table 1. Types with the suffix “float” indicate the statistic is related to the floating IP address while the “back” suffix indicates the statistic related to the background IP address.

Table 1: DoS Traffic Flow Sub-Index Types

kerberosback	enetmulticastunknown	rtcp
mobile	icmpback	espxgcp
enetunknown	udpunkown	debug
enetbroadcastunknown	arp	ikeback
xgcp	other	esptftp
tftp	mirror	kerberosfloat
snmp	ikefloat	ntp
sctp	ipunknown	rtp
icmpfloat	enetunicastunknown	dns

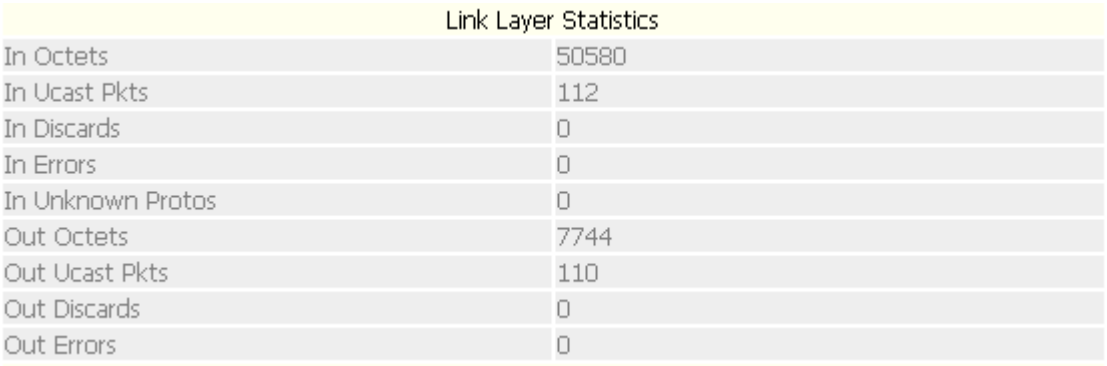


Figure 109. Ethernet Link Layer Statistics

In Octets

The total number of octets received on the interface, including framing characters.

In Ucast Pkts

The number of packets, delivered by this sub-layer to a higher layer, which were not addressed to a multicast or broadcast address at this sub-layer.

In Discards

The number of inbound packets discarded even though no errors were detected to prevent delivery to a higher-layer protocol.

In Errors

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

In Unknown Protos

The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

Out Octets

The total number of octets transmitted out of the interface, including framing characters.

Out Ucast Pkts

The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

Out Discards

The number of outbound packets discarded even though no errors had been detected to prevent transmission.

Out Errors

The number of outbound packets that could not be transmitted because of errors.

BITS Status

The following section discusses how to monitor BITS status and provides brief descriptions of each parameter or statistic.

To view BITS parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 110.

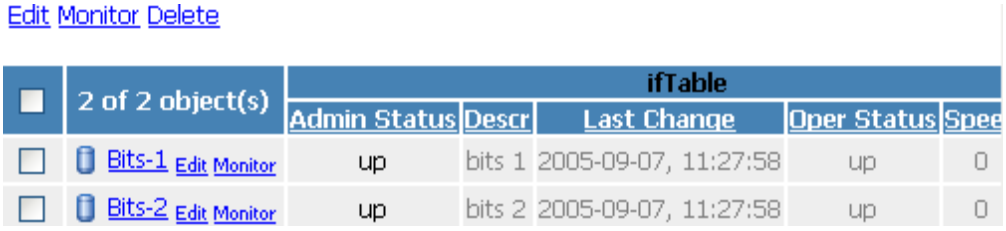


Figure 110. Interfaces Table (BITS shown)

2. Select the **Monitor** link to the right of the **Bits-n** link to display the corresponding information, as shown Figure 111.

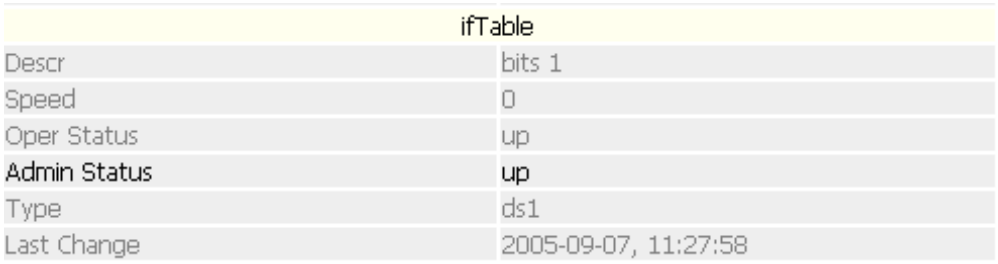


Figure 111. BITS General Statistics

Descr

Nuera's name for the interface.

Speed

The maximum bandwidth in bits per second.

Oper Status

The current operational status of the interface.

The BITS clock Oper Status may remain down until it has been assigned as a NetRef. See "Configuring NetRef" on page 39.

Admin Status

The desired state of the interface.

Type

The type of interface.

Last Change

The timestamp marking the last change to Oper Status.

DS3 Status

The following section discusses how to monitor DS3 status and provides brief descriptions of each parameter or statistic.

To view DS3 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 112.

	3 of 3 object(s)	Mac Assignment 1	Mac Assignment 2	Mac Assignment 3
☐	Ds3-1 Edit Monitor	1	none	3
☐	Ds3-2 Edit Monitor	1	none	3
☐	Ds3-3 Edit Monitor	1	2	none

Figure 112. Interfaces Table (DS3 Shown)

2. Select the **Monitor** link to the right of the **DS3-n** link to display the corresponding information. The table displayed has been broken up in the following figures and sections (shown in order) to improve readability.

MGC Assignments

For an explanation of the MGC Assignments as shown in Figure 113 see "To configure DS3s - MGC Assignments:" on page 52.

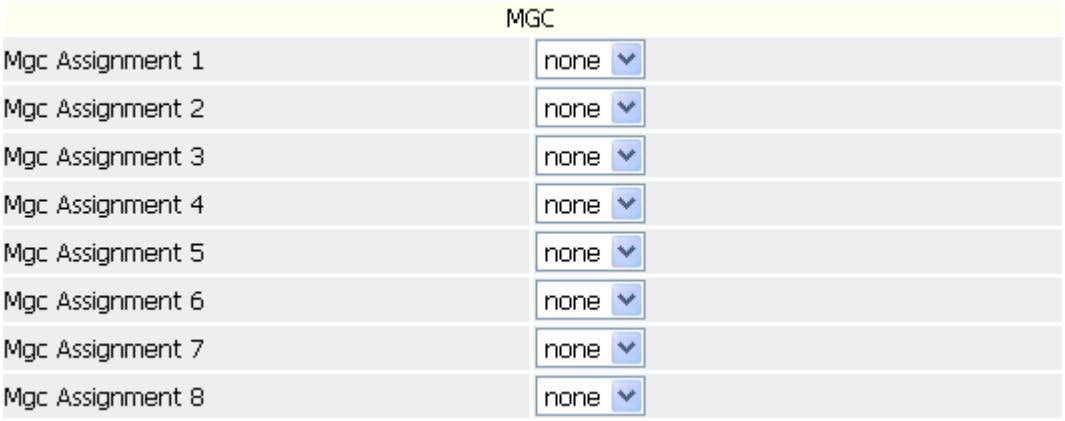


Figure 113. DS3 MGC Assignments

ds3ConfigTable

For an explanation of the DS3 configuration parameters as shown in Figure 114 see "To configure DS3s - DS3 Config Section:" on page 53.

Figure 114. DS3 ConfigTable

Time Elapsed

The number of seconds that have elapsed since the beginning of the near end current error-measurement period.

Valid Intervals

The number of previous near end intervals for which data was collected. The value will be 96 unless the interface was brought online within the last 24 hours, in which case the value will be the number of complete 15 minute near end intervals since the interface has been online.

Line Status

This variable indicates the Line Status of the interface. It contains loopback state information and failure state information.

Invalid Intervals

The number of intervals in the range from 0 to Valid Intervals for which no data is available. This will typically be zero.

Line Status Last Change

The time this DS3 entered its current line status state.

Loopback Status

This variable represents the current state of the loopback on the DS3 interface.

dsx3CurrentTable and ds3TotalTable

The DSx3CurrentTable and dsx3TotalTable have the same statistics. Their statistics are listed in different order.

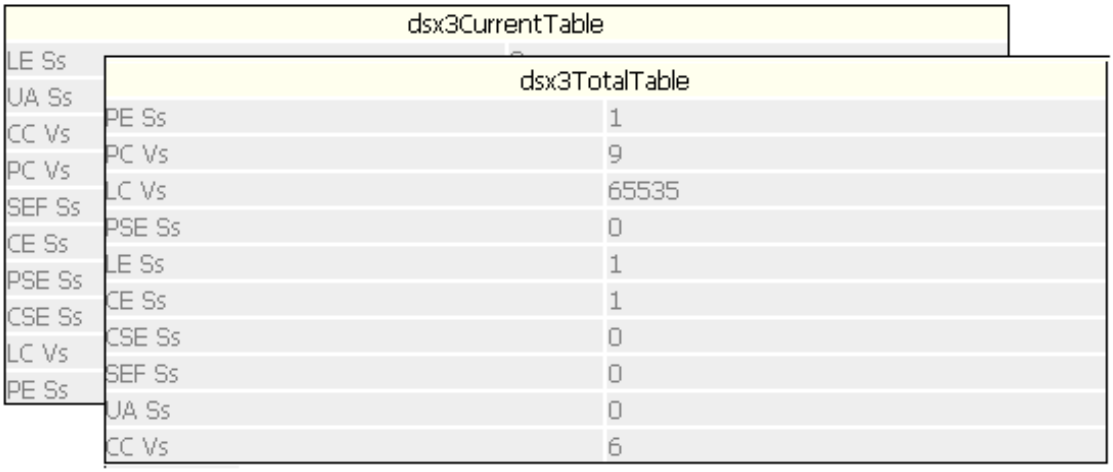


Figure 115. DS3 Current, Interval, and Total Tables

LESs

The number of Line Errored Seconds.

UASs

The counter associated with the number of Unavailable Seconds.

CCVs

The number of C-bit Coding Violations.

PCVs

The counter associated with the number of P-bit Coding Violations.

SEFSs

The counter associated with the number of Severely Errored Framing Seconds.

CESs

The number of C-bit Errored Seconds.

PSESs

The counter associated with the number of P-bit Severely Errored Seconds.

CSESs

The number of C-bit Severely Errored Seconds.

LCVs

The counter associated with the number of Line Coding Violations.

PESs

The counter associated with the number of P-bit Errored Seconds.

ifTable, mgcConfigTable, n4kIFStatsTable

For an explanation of the configuration parameters as shown in Figure 116 see "To configure DS3s - ifTable, mgcConfigtable, and StatsTable:" on page 54.

ifTable	
Descr	ds3-1
Type	ds3
Speed	44736000
Admin Status	up
Oper Status	testing
Last Change	2007-01-10, 03:23:24
n4kIfStatsTable	
Clear	noop
Calls In Progress	0
Calls Blocked	0
Clear Call Blocked	noop

Figure 116. DS3 ifTable and n4kIfStatsTable

Descr

A text string describing the interface.

Type

The type of interface.

Speed

An estimate of the interface's current bandwidth in bits per second.

Admin Status

The desired state of the interface.

Oper Status

The current operational state of the interface.

Last Change

The date and time of the last change to this interface.

Calls in Progress

Indicates total number of calls in progress since the last poll.

Calls Blocked

Indicates the total number of calls being blocked at the time of poll.

Clear Call Blocked

Resets the call blocked counter for this interface.

OC3 Status

The following section discusses how to monitor OC3 status and provides brief descriptions of each parameter or statistic.

To view OC3 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 117.

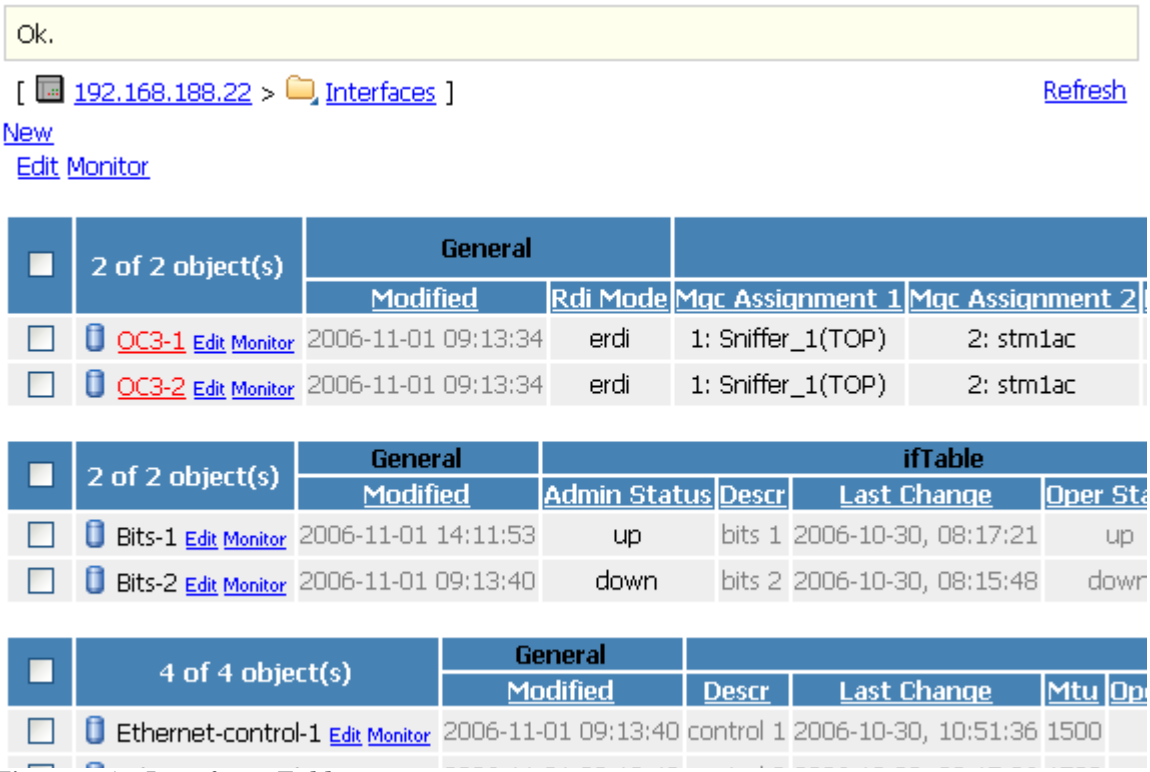


Figure 117. Interfaces Table

2. Select **Monitor** to the right of the **OC3-1** link to display the corresponding information.

MGC Assignments

For an explanation of the MGC Assignments as shown in Figure 118 see "To configure DS3s - MGC Assignments:" on page 52.

Modified	2006-10-24 10:31:31
Rdi Mode	erdi
MGC	
Mgc Assignment 1	1: Sniffer_1(top)
Mgc Assignment 2	2: stm1ac
Mgc Assignment 3	3: Linux Jammer .50
Mgc Assignment 4	4: MAC Script PC
Mgc Assignment 5	5: Linux Jammer .52
Mgc Assignment 6	6: Linux Jammer .53
Mgc Assignment 7	7: Linux Server .54
Mgc Assignment 8	9: Chris
Hunt	disable
APS Config	
Switch	noCmd
APS Status	
K1 K2 Rcv	0110
K1 K2 Trans	0110
Current	noErrors
Mode Mismatches	0
Channel Mismatches	0
PSBFs	0
FEPLFs	0
Switched Channel	0
Discontinuity Time	0
Group Status Last Switchover	2006-10-16, 12:50:45
Group Status Traffic Channel	OC3-2/APSGroup-Working-1
Group Status Switch Command	noCmd

Refresh Auto Off (Auto) Cancel

Figure 118. OC3 Interface Parameters and Statistics

K1 K2 Rcv

The current value of the K1 and K2 bytes received on the protection channel.

K1 K2 Trans

The current value of the K1 and K2 bytes transmitted on the protection channel.

Current

The current status of the APS group. This can be one of the following: APS mode mismatch or Protection Switch Byte Failure.

Mode Mismatches

This counter displays the number of conflicts between the current local mode and the received K2 mode information. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value Discontinuity Time, as described below.

Channel Mismatches

This counter indicates that a mismatch between the transmitted K1 channel and the received K2 channel has been detected. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value of Discontinuity Time, as described below.

PSBFs

This counter indicates a Protection Switch Byte Failure (PSBF) is in effect. This condition occurs when either an inconsistent APS byte or an invalid code is detected. An inconsistent APS byte occurs when no three consecutive K1 bytes of the last 12 successive frames are identical, starting with the last frame containing a previously consistent byte. An invalid code occurs when the incoming K1 byte contains an unused code or a code irrelevant for the specific switching operation (e.g., Reverse Request while no switching request is outstanding) in three consecutive frames. An invalid code also occurs when the incoming K1 byte contains an invalid channel number in three consecutive frames.

FEPLFs

A count of Far-End Protection-Line Failure conditions. This condition is declared based on receiving SF on the protection line in the K1 byte. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value of apsStatusDiscontinuityTime.

Switched Channel

The number of the channel currently switched to protection. The value 0 indicates no channel is switched to protection. The value 1 indicates that the working channel has switched to protection.

Discontinuity Time

The value of sysUpTime on the most recent occasion at which any one or more of this APS group's counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the system or interface, then this object contains a zero value.

Group Status Last Switchover

This parameter reports the time of the last switchover.

Group Status Traffic Channel

This reports the current traffic bearing channel.

Group Status Switch Command

This reports if the switch command was successful.

OC3 Working and Protect Interface Status

The following section discusses how to monitor OC3 Working and Protect Interface status and provides brief descriptions of each parameter or statistic.

To view OC3 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 119.

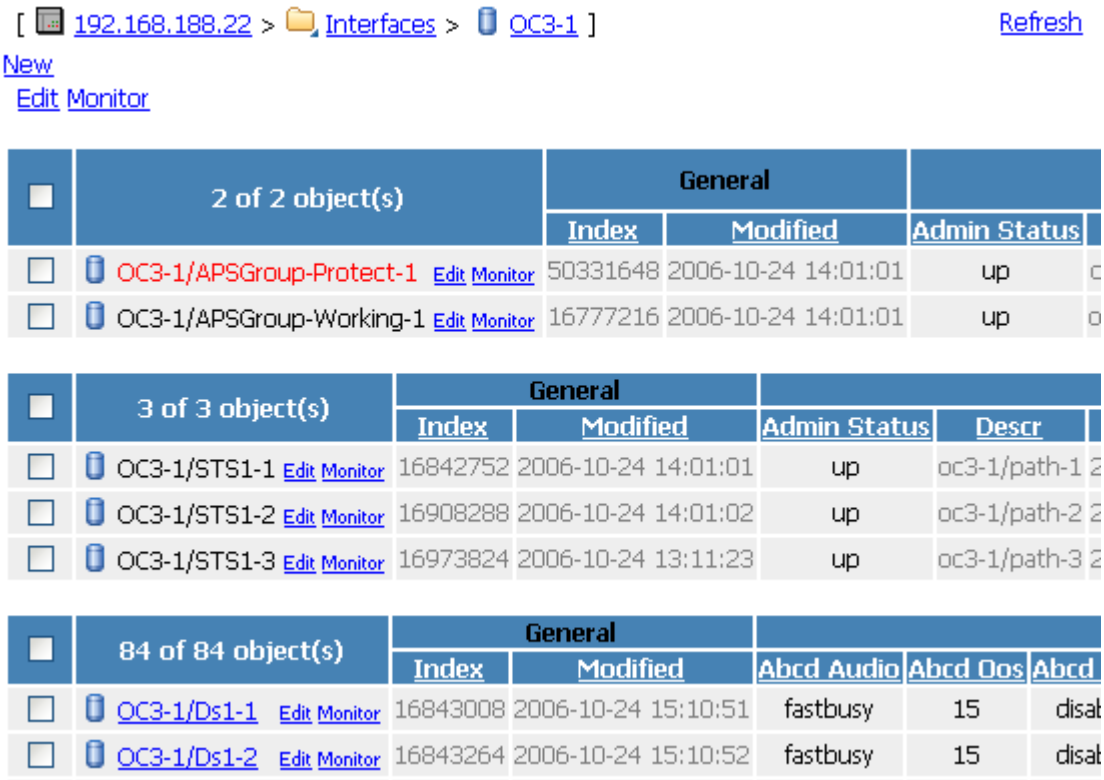
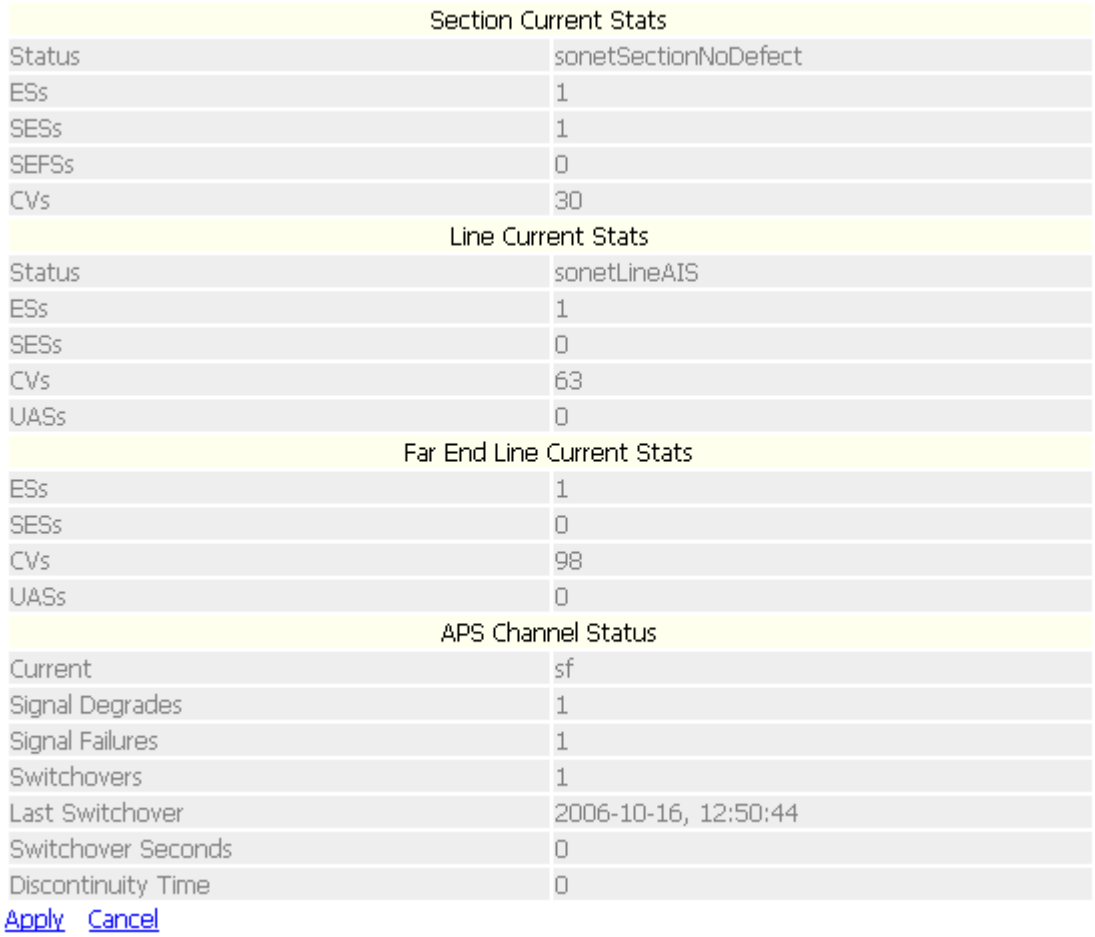


Figure 119. OC3 Interface Objects

2. Select **Monitor** to the right of the **OC3-1/APSGroup-Working-1** link to display the corresponding information.



Section Current Stats	
Status	sonetSectionNoDefect
ESs	1
SESs	1
SEFSs	0
CVs	30
Line Current Stats	
Status	sonetLineAIS
ESs	1
SESs	0
CVs	63
UASs	0
Far End Line Current Stats	
ESs	1
SESs	0
CVs	98
UASs	0
APS Channel Status	
Current	sf
Signal Degrades	1
Signal Failures	1
Switchovers	1
Last Switchover	2006-10-16, 12:50:44
Switchover Seconds	0
Discontinuity Time	0

Apply Cancel

Figure 120. OC3 Working Interface Statistics (cropped)

Status

This status provides information about the status of the interface at varying levels including failure state information.

ESs

The number of Errored Seconds.

SESs

The number of Severely Errored Seconds.

SEFSs

The number of Severely Errored Framing Seconds.

CVs

The number of Coding Violations.

UASs

The number of Unavailable Seconds.

APS Channel Status

Current

The current state of the port. The possible states are:

- **lockedOut** indicates that this bit, when applied to a working channel, indicates that the channel is prevented from switching to the protection line. When applied to the null channel, this bit indiates that no working channel may switch to the protection line.
- **sd** indicates a signal degrade condition is in effect.
- **sf** indicates a signal failure condition is in effect.
- **switched** indicates that the switch bit is applied to a working channel if that channel is currently switched to the protection line.
- **wtr** indicates that a wait-to-restore state is in effect.

Signal Degrades

A count of Signal Degrade conditions. This condition occurs when the line Bit Error Rate exceeds the currently configured value of the relevant instance of apsConfigSdBerThreshold.

Signal Failures

A count of Signal Failure conditions that have been detected on the incoming signal. This condition occurs when a loss of signal, loss of frame, AIS-L or a Line bit error rate exceeding the currently configured value of the relevant instance of apsConfigSfBerThreshold.

Switchovers

A count of the number of times this channel has switched from the protection lineto the working line, or vice versa.

Last Switchover

The date and time of the last switchover.

Switchover Seconds

The cumulative Protection Switching Duration (PSD) time in seconds. For a working channel, this is the cumulative number of seconds that service was carried on the protection line. For the protection line, this is the cumulative number of seconds that the protection line has been used to carry any working channel traffic. This information is only valid if revertive switching is enabled. The value 0 will be returned otherwise.

Discontinuity Time

The date and time of the most recent occassion at which any one or more of this channel's counters suffered a discontinuity.

STS1 Status

The following section discusses how to monitor STS1 status and provides brief descriptions of each parameter or statistic.

To view STS1 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 121.

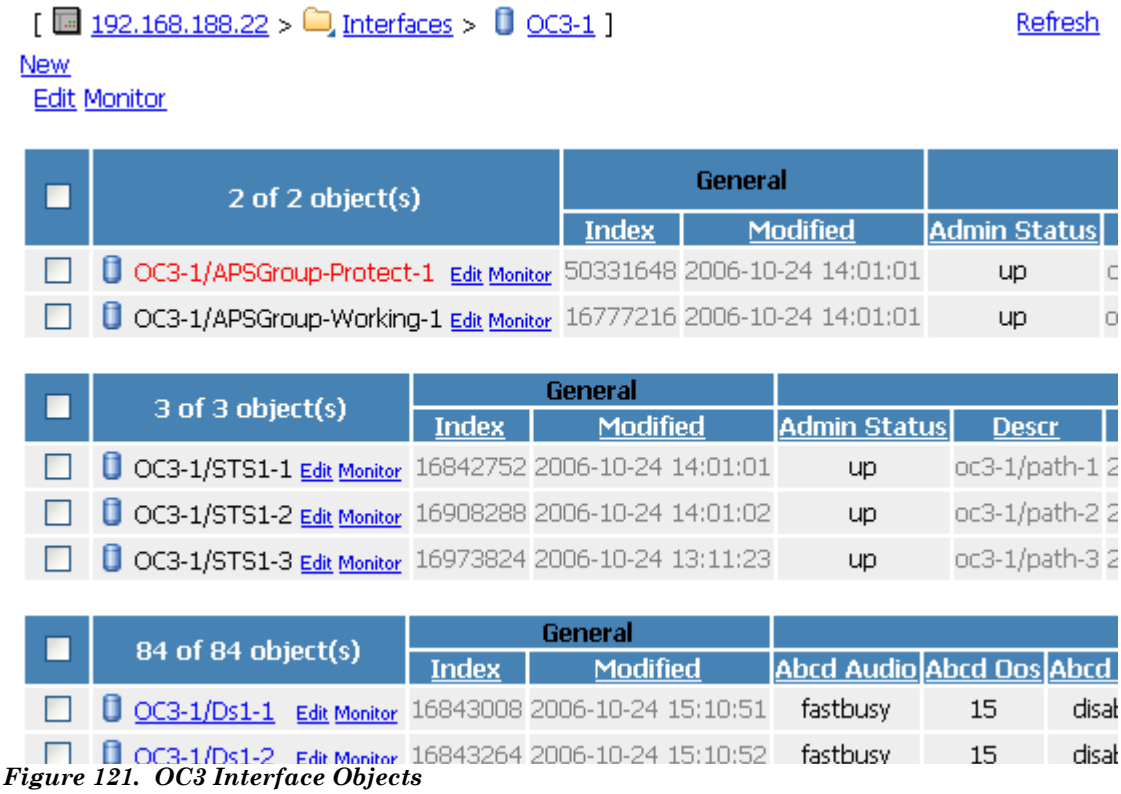


Figure 121. OC3 Interface Objects

2. Select **Monitor** to the right of the **OC3-1/STS1-1** link to display the corresponding information.

Modified	2006-10-24 14:01:01
Index	16842752
ifTable	
Descr	oc3-1/path-1
Type	sonetPath
Speed	51840000
Phys Address	
Admin Status	up
Oper Status	up
Last Change	2006-10-16, 12:50:46
sonetPathCurrentTable	
Width	sts1
Status	sonetPathNoDefect
ESs	2
SESs	2
CVs	0
UASs	0
sonetFarEndPathCurrentTable	
ESs	0
SESs	0
CVs	0
UASs	0
n4kIfStatsTable	
Clear All Sonet Stats	noop
Calls In Progress	0
Calls Blocked	0
Clear Call Blocked	noop
n4kSonetPathCurrentTable	
Current Status Last Change	2006-10-24, 12:45:58
Circuit Identifier	

Figure 122. STS1 Interface Statistics

Descr

A text string containing information about the interface.

Type

The type of interface.

Speed

An estimate of the interface's current bandwidth in bits per second.

Phys Address

The physical address of the interface.

Oper Status

The operational status of the interface.

Last Change

The date and time of the last change to the operational status.

Width

The description of SONET path, in this case, STS1.

Status

This status provides information about the status of the interface at varying levels including failure state information.

ESs

The number of Errored Seconds.

SESs

The number of Severely Errored Seconds.

CVs

The number of Coding Violations.

UASs

The number of Unavailable Seconds.

Calls in Progress

Indicates the total number of calls in progress sincethelast poll.

Calls Blocked

Indicates the total number of calls being blocked at the time of the poll.

DS1 and E1 Status

The following section detail how to monitor DS1 and E1 status, and provides brief descriptions of each parameter or statistic. For simplicity, throughout these sections, E1 interfaces will be referred to as DS1 interfaces.

To view DS1 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > **DS3-n** (or **OC3-1**) to show the DS1 table shown in Figure 123.

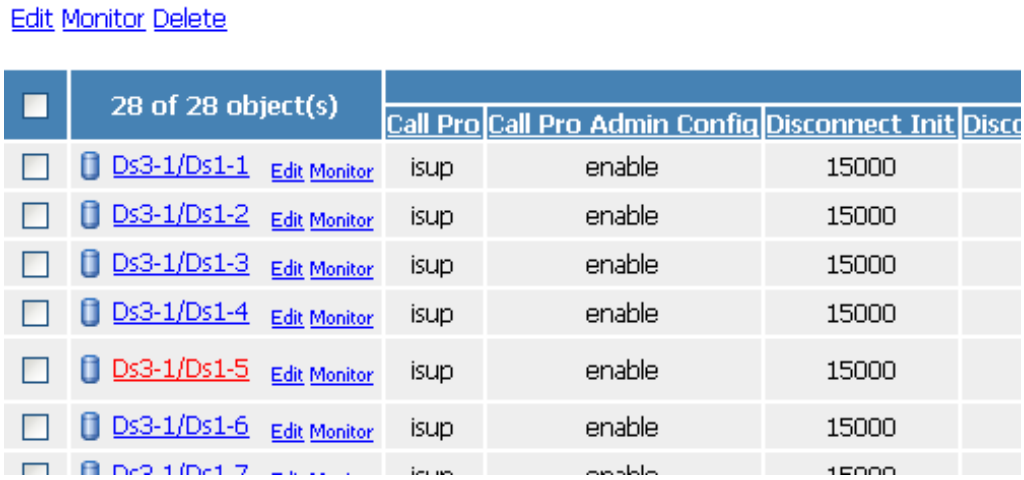

Edit Monitor Delete
28 of 28 object(s)
Call Pro
Call Pro Admin Config
Disconnect Init
Disco
Ds3-1/Ds1-1 Edit Monitor isup enable 15000
Ds3-1/Ds1-2 Edit Monitor isup enable 15000
Ds3-1/Ds1-3 Edit Monitor isup enable 15000
Ds3-1/Ds1-4 Edit Monitor isup enable 15000
Ds3-1/Ds1-5 Edit Monitor isup enable 15000
Ds3-1/Ds1-6 Edit Monitor isup enable 15000

Figure 123. DS1 Table

To improve readability, the statistical information tables that follow may be presented in a different order than they appear in NetConductor.

Media

For an explanation of the parameters shown in Figure 124 see page 70.

Media	
Gain Enc	0
Gain Dec	0
Voice Codec	pcmUlaw64k10ms
Echo Enable	enabled
Echo Nlp Enable	enabled
Echo Tone Disabler	enabled
Vad Enable	none
Vad Threshold	-36
Vad Hangover	255
Compand	pcmUlaw
Fax Codec	none
Modem Codec	none
RFC2833 Payload	127
Dtmf Relay	enabled
Digit Level	-7

Figure 124. DS1 Media Assignments

MediaTGCP

For an explanation of the parameters shown in Figure 125 see page 72.

Media TGCP	
Call Pro Admin Config	disable
Call Pro	isup
Ip Tos	160
Initial Resend Delay	200
Max Resend Delay	5000
Hunt Resend Count	3
Disconnect Retransmits	10
Disconnect Init	15000
Disconnect Max	60000
Wildcard Rsip Enable	enabled
Piggyback Response Enable	enabled
Encryption Enable	enabled
Retransmit Timer Max	20000
Response History Length	30000
Xgcp Feature Config	0

Figure 125. DS1 Media TGCP Assignments

MediaTones (busy, dialtone, fastbusy, ringback, and warble)

For an explanation of parameters shown in Figure 126, see page 76.

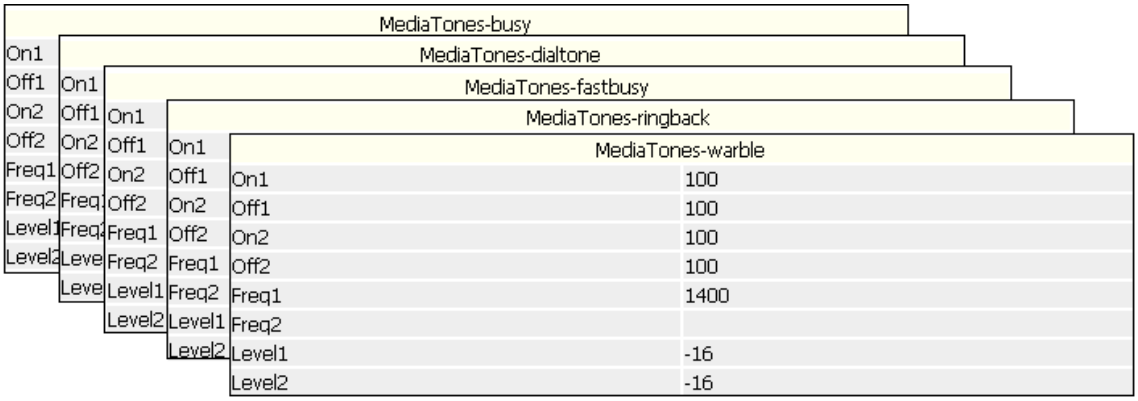


Figure 126. DS1 MediaTones Assignments

dsx1ConfigTable

For an explanation of the configuration parameters shown in Figure 127, see page 75.

dsx1ConfigTable	
Time Elapsed	406
Valid Intervals	96
Line Type	dsx1ESF
Circuit Identifier	
Loopback Config	dsx1NoLoop
Line Status	dsx1NoAlarm
Signal Mode	none
Invalid Intervals	96
Line Status Last Change	2005-01-23, 07:40:30
Loopback Status	dsx1NoLoopback

Figure 127. DS1ConfigTable

Time Elapsed

The number of seconds that have elapsed since the beginning of the near end current error-measurement period.

Valid Intervals

The number of previous near end intervals for which data was collected. The value will be 96 unless the interface was brought online within the last 24 hours, in which case the value will be the number of complete 15 minute near end intervals since the interface has been online.

Line Status

This variable indicates the Line Status of the interface. It contains loopback state information and failure state information.

Invalid Intervals

The number of intervals in the range from 0 to Valid Intervals for which no data is available. This will typically be zero.

Line Status Last Change

The time this DS1 entered its current line status state.

Loopback Status

This variable represents the current state of the loopback on the DS1 interface.

ifTable, n4kIFStatsTable

For an explanation of the configuration parameters shown in Figure 128, see page 77.

ifTable	
Descr	ds3-2/ds1-1
Type	ds1
Speed	1544000
Admin Status	down
Oper Status	down
Last Change	1203
n4kIfStatsTable	
Clear	noop
Calls In Progress	0
Calls Blocked	0
Clear Call Blocked	noop

Figure 128. DS1 ifTable and n4kIfStatsTable

Descr

A text string containing information about the interface.

Type

The type of interface.

Speed

An estimate of the interface's current bandwidth in bits per second.

Oper Status

The operational status of the interface.

Last Change

The date and time of the last change to the operational status of the interface.

Calls in Progress

The number of calls currently in progress on this interface.

Calls Blocked

The number of calls blocked on this interface.

dsx1CurrentTable and ds1TotalTable

Although presented in a different order, the DSx1CurrentTable and dsx1TotalTable display the same statistics.

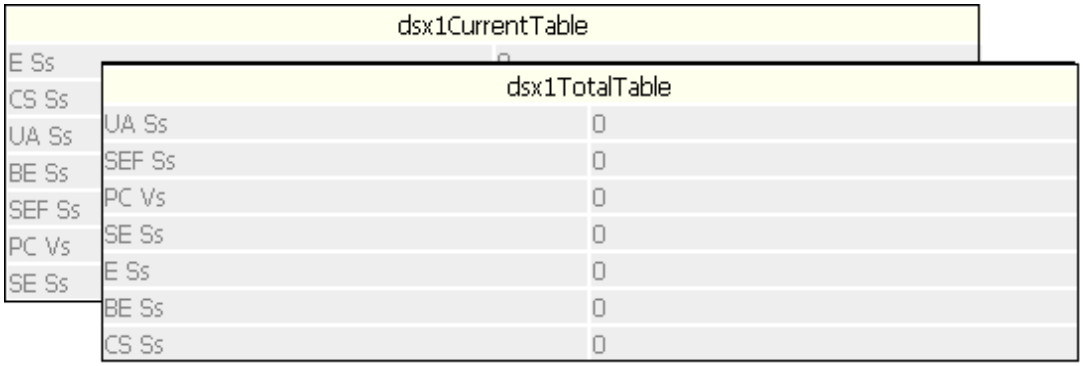


Figure 129. DS1 Statistics Tables

ESs

The number of Errored Seconds.

CSSs

The number of Controlled Slip Seconds.

UASs

The number of Unavailable Seconds.

BESs

The number of Bursty Errored Seconds.

SEFSs

The number of Severely Errored Framing Seconds.

PCVs

The number of Path Coding Violations.

SESs

The number of Severely Errored Seconds.

STM-1 Status

The following section discusses how to monitor STM-1 status and provides brief descriptions of each parameter or statistic.

To view STM-1 parameters and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 130.

	2 of 2 object(s)					APS Status
		Channel Mismatches	Current	Discontinuity Time	FEPL Fs	K1 K2 Rcv
☐	STM1-1 Edit Monitor	0	0	0	0	0000
☐	STM1-2 Edit Monitor	0	0	0	0	0000

Edit Monitor Delete

Figure 130. Interface Table (STM-1 shown)

2. Select **Monitor** to the right of the **STM-1**to display the corresponding information, as shown Figure 131.

APS Config	
Switch	forcedSwitchProtectToWork
APS Status	
K1 K2 Rcv	ad77
K1 K2 Trans	e110
Current	psbf
Mode Mismatches	0
Channel Mismatches	0
PSBFs	7
FEPLFs	0
Switched Channel	0
Discontinuity Time	0
Group Status Last Switchover	2006-08-29, 08:34:44
Group Status Traffic Channel	STM1-1/APSGroup-Working-1
Group Status Switch Command	successful
MGC	
Hunt	enable
Mgc Assignment 1	3: MGCTemplat
Mgc Assignment 2	10: MGCTemplat
Mgc Assignment 3	1: MGCTemplat
Mgc Assignment 4	2: MGCTemplat
Mgc Assignment 5	3: MGCTemplat
Mgc Assignment 6	5: MGCTemplat
Mgc Assignment 7	9: MGCTemplat
Mgc Assignment 8	24: MGCTemplat

Figure 131. STM-1 General Statistics

APS Status

K1 K2 Rcv

The current value of the K1 and K2 bytes received on the protection channel.

K1 K2 Trans

The current value of the K1 and K2 bytes transmitted on the protection channel.

Current

The current status of the APS group. This can be one of the following: APS mode mismatch or Protection Switch Byte Failure.

Mode Mismatches

This counter displays the number of conflicts between the current local mode and the received K2 mode information. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value Discontinuity Time, as described below.

Channel Mismatches

This counter indicates that a mismatch between the transmitted K1 channel and the received K2 channel has been detected. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value of Discontinuity Time, as described below.

PSBFs

This counter indicates a Protection Switch Byte Failure (PSBF) is in effect. This condition occurs when either an inconsistent APS byte or an invalid code is detected. An inconsistent APS byte occurs when no three consecutive K1 bytes of the last 12 successive frames are identical, starting with the last frame containing a previously consistent byte. An invalid code occurs when the incoming K1 byte contains an unused code or a code irrelevant for the specific switching operation (e.g., Reverse Request while no switching request is outstanding) in three consecutive frames. An invalid code also occurs when the incoming K1 byte contains an invalid channel number in three consecutive frames.

FEPLFs

A count of Far-End Protection-Line Failure conditions. This condition is declared based on receiving SF on the protection line in the K1 byte. Discontinuities in the value of this counter can occur when the management system is reinitializated or at other times as indicated by the value of apsStatusDiscontinuityTime.

Switched Channel

The number of the channel currently switched to protection. The value 0 indicates no channel is switched to protection. The value 1 indicates that the working channel has switched to protection.

Discontinuity Time

The value of sysUpTime on the most recent occasion at which any one or more of this APS group's counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the system or interface, then this object contains a zero value.

Group Status Last Switchover

This parameter reports the time of the last switchover.

Group Status Traffic Channel

This reports the current traffic bearing channel.

Group Status Switch Command

This reports if the switch command was successful.

STM-1 Working and Protect Interface Status

The following section discusses how to monitor STM-1 Working and Protect Interface status and provides brief descriptions of each parameter or statistic.

To view OC3 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 132.

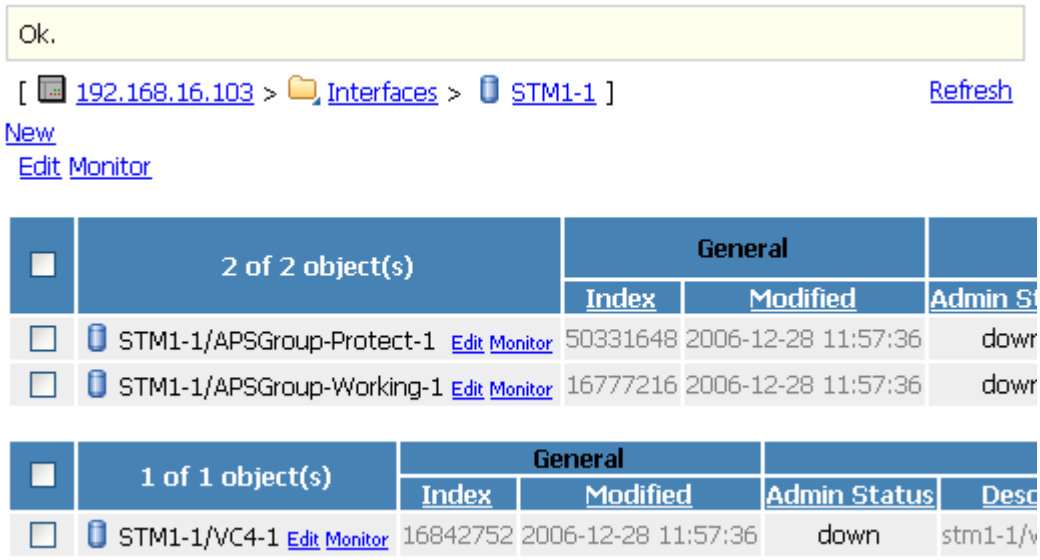
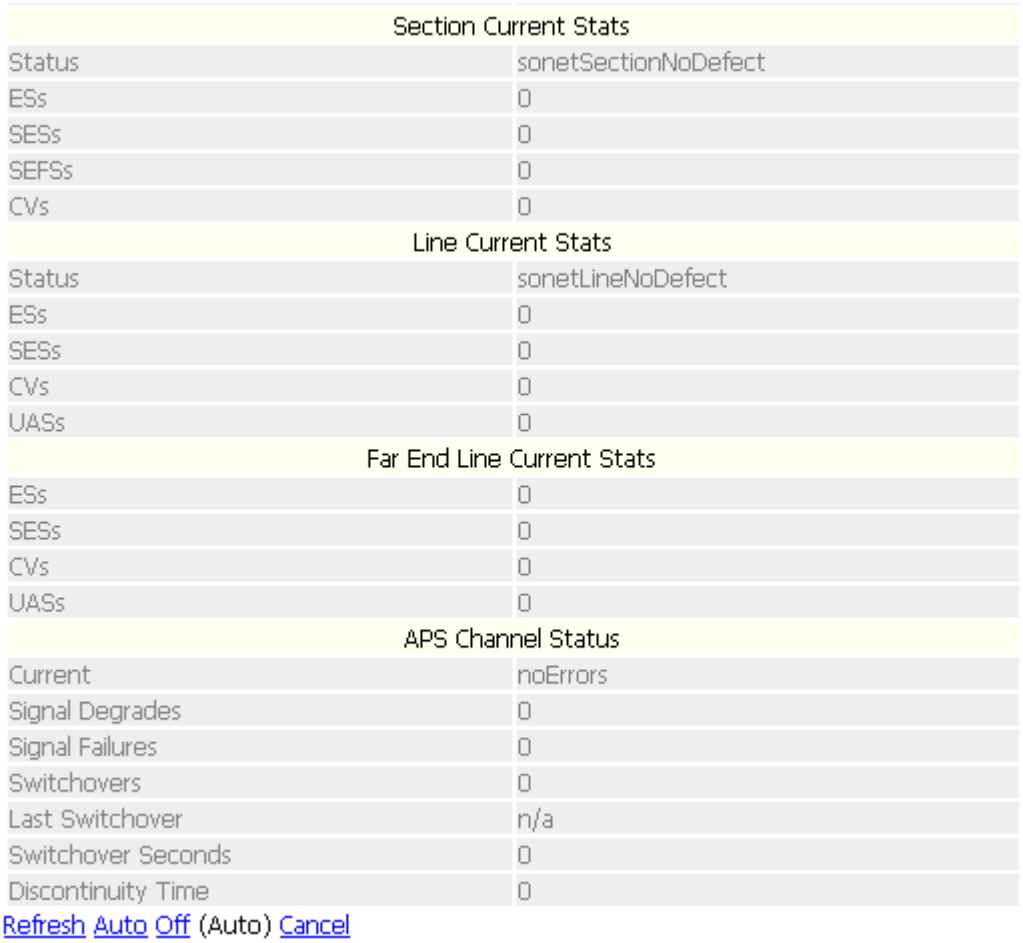


Figure 132. STM-1 Interface Objects

2. Select **Monitor** to the right of the **STM-1/APSGroup-Working-1** link to display the corresponding information.



Section Current Stats	
Status	sonetSectionNoDefect
ESs	0
SESs	0
SEFSs	0
CVs	0
Line Current Stats	
Status	sonetLineNoDefect
ESs	0
SESs	0
CVs	0
UASs	0
Far End Line Current Stats	
ESs	0
SESs	0
CVs	0
UASs	0
APS Channel Status	
Current	noErrors
Signal Degrades	0
Signal Failures	0
Switchovers	0
Last Switchover	n/a
Switchover Seconds	0
Discontinuity Time	0

Figure 133. STM-1 Working Interface Statistics (cropped)

Status

This status provides information about the status of the interface at varying levels including failure state information.

ESs

The number of Errored Seconds.

SESs

The number of Severely Errored Seconds.

SEFSs

The number of Severely Errored Framing Seconds.

CVs

The number of Coding Violations.

UASs

The number of Unavailable Seconds.

APS Channel Status

Current

The current state of the port. The possible states are:

- **lockedOut** indicates that this bit, when applied to a working channel, indicates that the channel is prevented from switching to the protection line. When applied to the null channel, this bit indiates that no working channel may switch to the protection line.
- **sd** indicates a signal degrade condition is in effect.
- **sf** indicates a signal failure condition is in effect.
- **switched** indicates that the switch bit is applied to a working channel if that channel is currently switched to the protection line.
- **wtr** indicates that a wait-to-restore state is in effect.

Signal Degrades

A count of signal degrade conditions. This condition occurs when the line Bit Error Rate exceeds the currently configured value of the relevant instance of apsConfigSdBerThreshold.

Signal Failures

A count of signal failure conditions that have been detected on the incoming signal. This condition occurs when a loss of signal, loss of frame, AIS-L or a Line bit error rate exceeding the currently configured value of the relevant instance of apsConfigSfBerThreshold.

Switchovers

A count of the number of times this channel has switched from the protection lineto the working line, or vice versa.

Last Switchover

The date and time of the last switchover.

Switchover Seconds

The cumulative Protection Switching Duration (PSD) time in seconds. For a working channel, this is the cumulative number of seconds that service was carried on the protection line. For the protection line, this is the cumulative number of seconds that the protection line has been used to carry any working channel traffic. This information is only valid if revertive switching is enabled. The value 0 will be returned otherwise.

Discontinuity Time

The date and time of the most recent occassion at which any one or more of this channel's counters suffered a discontinuity.

VC4 Status

The following section discusses how to monitor VC4 status and provides brief descriptions of each parameter or statistic.

To view VC4 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** to view the table shown in Figure 134.

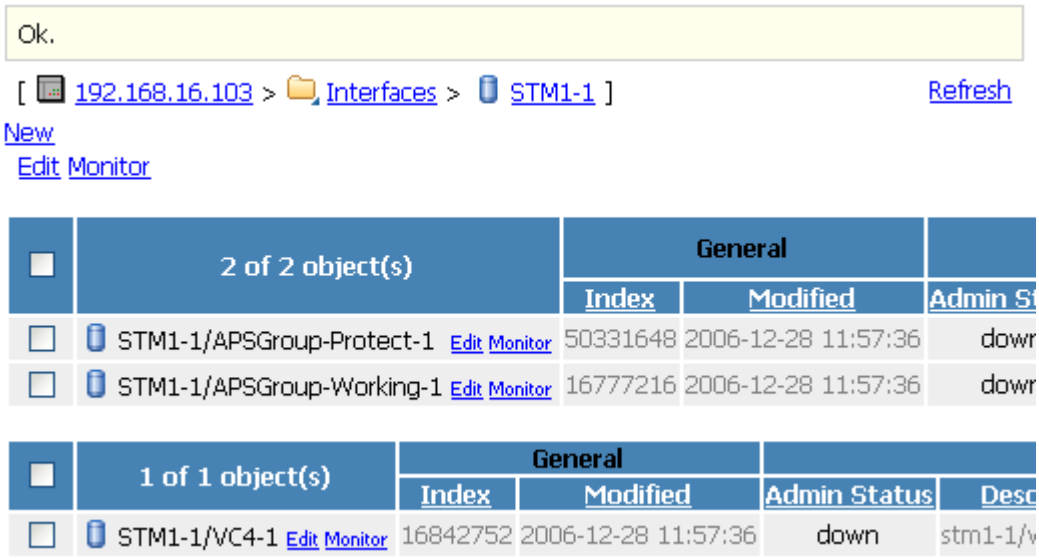


Figure 134. STM1/VC4 Interface Objects

2. Select **Monitor** to the right of the **STM1-1/VC4-1** link to display the corresponding information.

ifTable	
Descr	stm1-1/vc4-1
Type	sonetPath
Speed	150336000
Phys Address	
Admin Status	down
Oper Status	down
Last Change	2006-07-27, 09:47:09
sonetPathCurrentTable	
Width	sts3cSTM1
Status	sonetPathNoDefect
ESs	0
SESs	0
CVs	0
UASs	0
sonetFarEndPathCurrentTable	
ESs	0
SESs	0
CVs	0
UASs	0
n4kIfStatsTable	
Clear All Sonet Stats	noop
Calls In Progress	0
Calls Blocked	0
Clear Call Blocked	noop
n4kSonetPathCurrentTable	
Current Status Last Change	n/a
Circuit Identifier	

Figure 135. VC4 Interface Statistics

Descr

A text string containing information about the interface.

Type

The type of interface.

Speed

An estimate of the interface's current bandwidth in bits per second.

Phys Address

The physical address of the interface.

Oper Status

The operational status of the interface.

Last Change

The date and time of the last change to the operational status.

Width

The description of SONET path, in this case, sts3cSTM1.

Status

This status provides information about the status of the interface at varying levels including failure state information.

ESs

The number of Errored Seconds.

SESs

The number of Severely Errored Seconds.

CVs

The number of Coding Violations.

UASs

The number of Unavailable Seconds.

Calls in Progress

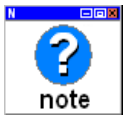
Indicates the total number of calls in progress sincethelast poll.

Calls Blocked

Indicates the total number of calls being blocked at the time of the poll.

DS0 Status

The following section discusses how to monitor DS0 status and provides brief descriptions of each parameter or statistic.



Individual statistics are cumulative for the DS0, rather than per call.

To view DS0 options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Interfaces** > TDM Interface > TDM Interface**/Ds1-n** to show the table shown in Figure 136.

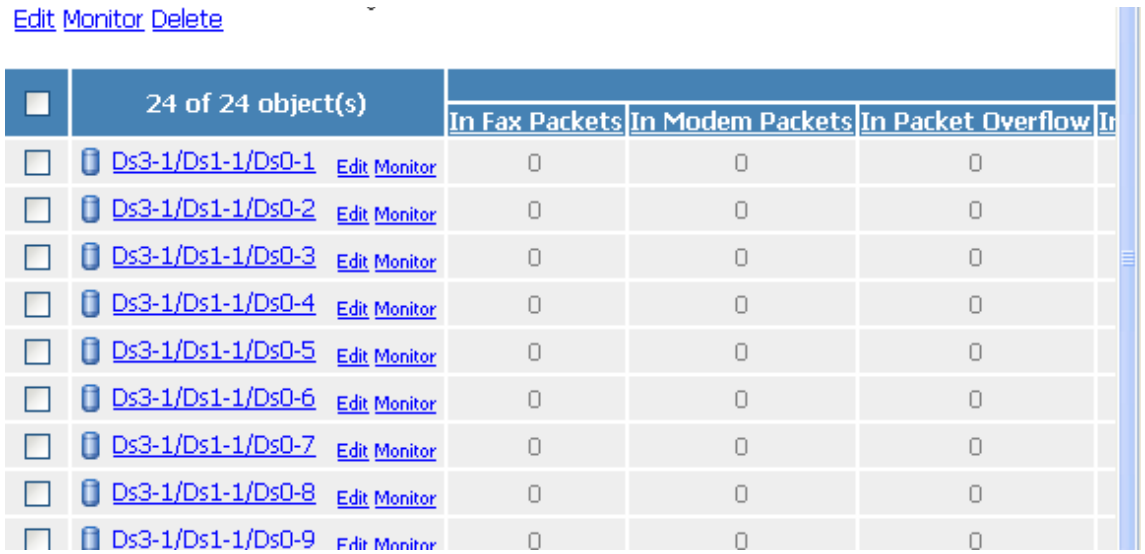


Figure 136. DS0 Information pane

2. Select the **Monitor** link to the right of the link to display the corresponding information. The table displayed has been broken up in the following figures and sections to improve readability.

	Statistics
In Total Packets	0
Out Total Packets	70293
In Rtp Media Packets	0
Out Rtp Media Packets	598
In Rtp Rfc2833 Packets	0
Out Rtp Rfc2833 Packets	0
In Fax Packets	0
Out Fax Packets	0
In Modem Packets	0
Out Modem Packets	0
In Rtcp Packets	0
Out Rtcp Packets	69699
In Xgcp Packets	0
Out Xgcp Packets	0
In Packet Overflow	0
Out Packet Overflow	0
Local Packet Loss	0
Remote Packet Loss	0
Rtp Auth Failures	0
Rtcp Auth Failures	0
In Rtp Unknown Packets	0
Echo Divergences	0

Figure 137. DS0 Statistics

In Total Packets

Indicates total number of packets received.

Out Total Packets

Indicates total number of packets sent.

In Rtp Media Packets

Indicates total number of RTP voice packets received.

Out Rtp Media Packets

Indicates total number of RTP voice packets sent.

In Rtp Rfc2833 Packets

Indicates total number of RFC2833 formatted packets received.

Out Rtp Rfc2833 Packets

Indicates total number of RFC2833 formatted packets sent.

In Fax Packets

Indicates total number of fax relay packets received.

Out Fax Packets

Indicates total number of fax relay packets sent.

In Modem Packets

Indicates total number of modem packets received.

Out Modem Packets

Indicates total number of modem packets sent.

In Rtcp Packets

Indicates total number of RTCP packets received.

Out Rtcp Packets

Indicates total number of RTCP packets sent.

In Xgcp Packets

Indicates total number of TGCP packets received.

Out Xgcp Packets

Indicates total number of TGCP packets sent.

In Packet Overflow

Indicates number of times the inbound packet queue overflowed.

Out Packet Overflow

Indicates number of times the outbound packet queue overflowed.

Local Packet Loss

Loss estimate according to local endpoint.

Remote Packet Loss

Loss estimate according to remote endpoint.

Rtp Auth Failures

The number of RTP Authentication failures during this call.

Rtcp Auth Failures

The number of RTCP Authentication failures during this call.

In Rtp Unknown Packets

The number of RTP packets received with an unknown payload type. This can also be considered a “dropped” RTP Packet count.

Echo Divergences

The number of times the echo canceller adaptive filter diverges. Divergence is expected during major signal and echo hybrid transitions (such as a change from voice to tones or during a call transfer) or when no echo is present in the signal (such as digital terminations).

Reset

This resets all statistics for the selected channel.

	Status
Codec	pcmu
Rate	64000
Packet Period	10
Echo	steady
Echo Erl	0
Echo Erle	0
Echo Tail Delay	0
Call Pro	idle
Abcd Enc	0
Abcd Dec	0
Local Jitter	0
Remote Jitter	0
Digits Src Enc	
Digits Dst Enc	
Digits Src Dec	
Digits Dst Dec	
Call Pro Mode	inactive
Call Pro Notified Entity	[0.0.0.0]:2727
Current Rtp Crypto	none
Current Rtcp Crypto	none
Current Rtp Auth	none
Current Rtcp Auth	none

Figure 138. DS0 Status

Codec

Indicates the current codec in use on the channel.

Rate

Indicates the current data rate in use on the channel, displayed in bits per second (bps).

Packet Period

Indicates the current packet period in use on the channel, if any.

Echo

Indicates current channel echo canceller status.

Echo ERL

The Echo Return Loss is the ratio between the signal energy sent towards the TDM subscriber and the echo energy received back from the TDM subscriber signal. This number is calculated prior to echo cancellation, expressed in dB.

Echo ERLE

The Echo Return Loss Enhancement is the amount of enhancement the echo canceller provides to the ERL, expressed in dB. This is the ratio between the echo canceller input signal and the echo canceller adaptive filter output signal, before NLP processing is applied.

Echo Tail Delay

The current estimate of the echo tail delay, expressed in (ms).

Call Pro

Call processing status.

Abcd Enc

ABCD bits, encoding from TDM to IP.

Abcd Dec

ABCD bits, decoding from IP to TDM.

Local Jitter

Indicates an estimate of the instantaneous local network jitter for the most recent completed call.

Remote Jitter

Indicates an estimate of the instantaneous remote network jitter for the most recent completed call.

Digits Scr Enc

Source digits encode from TDM to IP, ASCII.

Digits Dst Enc

Destination digits encode from TDM to IP, ASCII.

Digits Src Dec

Source digits decode from IP to TDM, ASCII.

Digits Dst Dec

Destination digits decode from IP to TDM, ASCII.

Call Pro Mode

Call processing mode, M: line of XGCP message.

Call Pro Notified Entity

IP:UDP of Current Call processing notified entity.

Current Rtp Crypto

RTP encryption algorithm used on this call.

Current Rtcp Crypto

RTCP encryption algorithm used on this call.

Current Rtcp Auth

RTCP authentication algorithm used on this call.

Current Rtcp Auth

RTCP authentication algorithm used on this call.

IPSec Template Status

The following section discusses how to monitor IPSec status and provides brief descriptions of each statistic.

To view IPSec statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/IPSec** to display the information pane shown in Figure 141.

	7 of 7 object(s)		General	
			Modified	IPSec Status
☐	IPSec Status-192.168.96.24/2728	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.96.25/2728	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.96.26/2728	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.98.210/2424	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.98.211/2424	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.98.212/2424	Edit Monitor	2006-06-25 10:50:22	down
☐	IPSec Status-192.168.98.213/2424	Edit Monitor	2006-06-25 10:50:22	down

Figure 139. IPSec Status

2. In the table, each IPSec tunnel is composed of the DNS resolved IP and the corresponding UDP port.
3. Select **Monitor** to the right of the appropriate **IPSec Status** to display the corresponding information, as shown Figure 142.

Invoked 'Monitor' action for 1 IPSec Status object(s).

[Yellowstone_Diego > Globals/IPSec > IPSec Status-192.168.96.24/2728] Refresh

Refresh Auto Off (Auto) Cancel

Modified	2006-06-25 10:50:22
IPSec Status	down

Refresh Auto Off (Auto) Cancel

Figure 140. IPSec Template Parameters and Status

IPSec Status

The current status of the IPSec tunnel. Up is secure.

DNS Server Status

The following section discusses how to monitor DNS Server status and provides brief descriptions of each parameter or statistic.

To view DNS Server options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **DNS**. The information window will show the table in Figure 141.

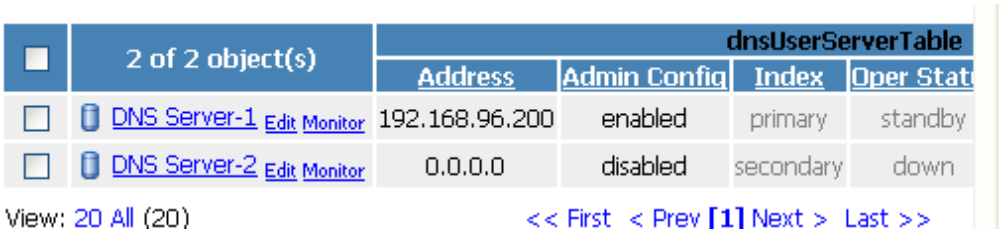


Figure 141. DNS Table

2. Select **Monitor** to the right of the appropriate **DNS Server** to display the corresponding information, as shown Figure 142.

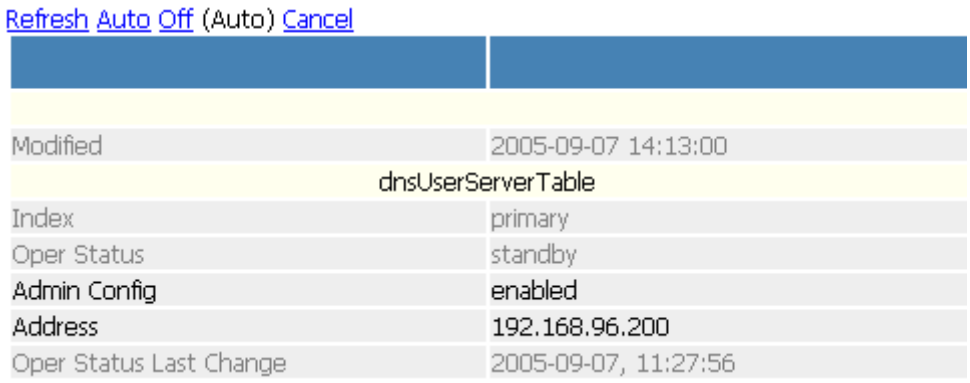


Figure 142. DNS Server Statistics

Index

The index of this DNS server.

Oper Status

The current operational state of the DNS server based on the outcome of the last query or, if no query, its Admin Config state.

Admin Config

The desired administrative configuration of the server.

Address

The IP network address of the DNS server.

Oper Status Last Change

The time when the DNS server operational status last changed.

DNS Resolver Status

You can view the DNS client's resolver cache under Globals/DNS.

To view DNS Resolver statistics:

1. Expand the hierarchy by selecting **Inventory**> [NE] > **Globals/DNS**. The information pane will display the table shown in Figure 143.

	1 of 1 object(s)	General	dnsUserMibObjects
		Modified	Clear Cache Op
☐	DNS Globals-1 Edit Monitor	2006-06-25 10:50:28	none

	22 of 22 object(s)	General	dnsUserResolve	
		Modified	Address	Fqdn
☐	DNS Resolver-1 Edit Monitor	2006-06-25 10:50:28	192.168.96.9	abcdefghijklmnopqrstuvv abcdefghijklmnopqrstuvv abcdefghi.rdt.nuera.cc
☐	DNS Resolver-2 Edit Monitor	2006-06-25 10:50:28	192.168.98.222	mesaverde.rdt.nuera.c
☐	DNS Resolver-3 Edit Monitor	2006-06-25 10:50:28	192.168.98.223	mesaverde.rdt.nuera.c
☐	DNS Resolver-4 Edit Monitor	2006-06-25 10:50:28	192.168.98.224	mesaverde.rdt.nuera.c
☐	DNS Resolver-5 Edit Monitor	2006-06-25 10:50:28	192.168.98.220	mesaverde.rdt.nuera.c
☐	DNS Resolver-6 Edit Monitor	2006-06-25 10:50:28	192.168.98.221	mesaverde.rdt.nuera.c
☐	DNS Resolver-7 Edit Monitor	2006-06-25 10:50:28	192.168.98.213	rockymountain.rdt.nuera
☐	DNS Resolver-8 Edit Monitor	2006-06-25 10:50:28	192.168.98.210	rockymountain.rdt.nuera

Figure 143. DNS Globals

2. Select **Monitor** to the right of the **DNS Resolver** to display the corresponding information pane, as shown in Figure 144.

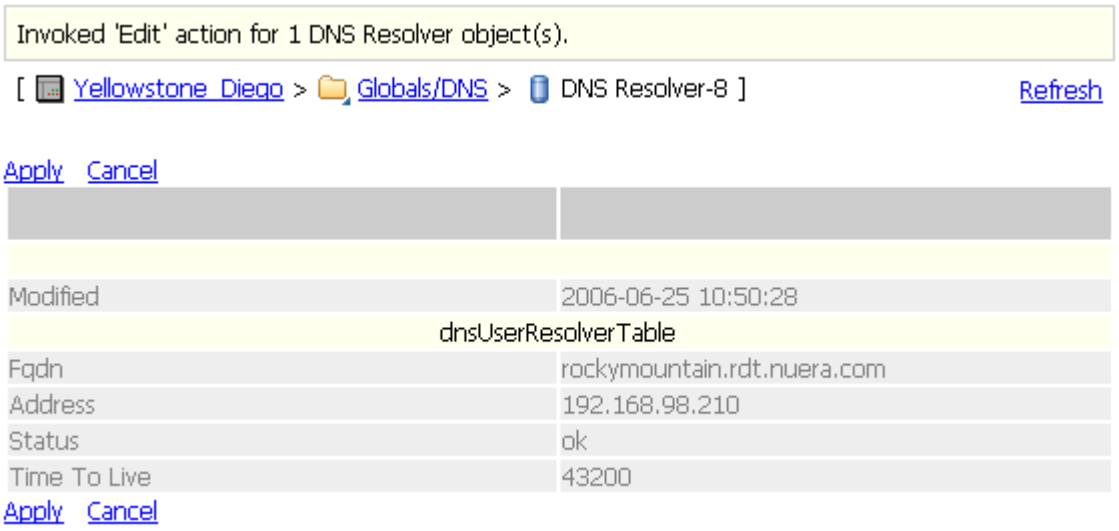


Figure 144. DNS Resolver Table

FQDN

The fully-qualified domain name of this cache entry.

Address

The resolved dot-quad IP address of this cache entry.

Status

The current status of this cache entry.

Time To Live

The time-to-live for this cache entry, measured in seconds.

NETREF Globals Status

Under NETREF globals, you can view the status of the current clock source, and initiate a switchover of the clock source.

To view NETREF Globals options and statistics:

1. Expand the hierarchy by selecting **Inventory**> [NE] > **Globals/NetRef**. The information pane will display the table shown in Figure 145.

	1 of 1 object(s)	General			netRefM
		Modified	Current Src	Current State	Source Last
☐	NetRef Globals-1 Edit Monitor	2007-01-11 15:26:51	Ds3-1/Ds1-1	holdover	2001-01-07,

Figure 145. NETREF Table

2. Select **Monitor** to the right of the **NetRef Globals** to display the corresponding system information, as shown Figure 146.

netRefMibObjects	
Switch Op	none
Current Src	Ds3-1/Ds1-1
Current State	holdover
Source Last Change	2001-01-07, 06:53:19
State Last Change	2001-01-07, 06:53:20

Refresh Auto Off (Auto) Cancel

Figure 146. NETREF Globals General Statistics

Switch Op

Performs a forced switchover of the current source of sync.

Current Src

Indicates which interface is the current source of sync.

Current State

Indicates the state of the current source of sync.

Source Last Change

The time when the current source of sync last changed.

State Last Change

The time when the current state of sync last changed.

Signaling Backhaul Parameters and Stats

SCTP Globals Status

The following section discusses how to monitor SCTP Globals status and provides brief descriptions of each parameter or statistic.

To view SCTP Globals options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** to view the table shown in Figure 147.

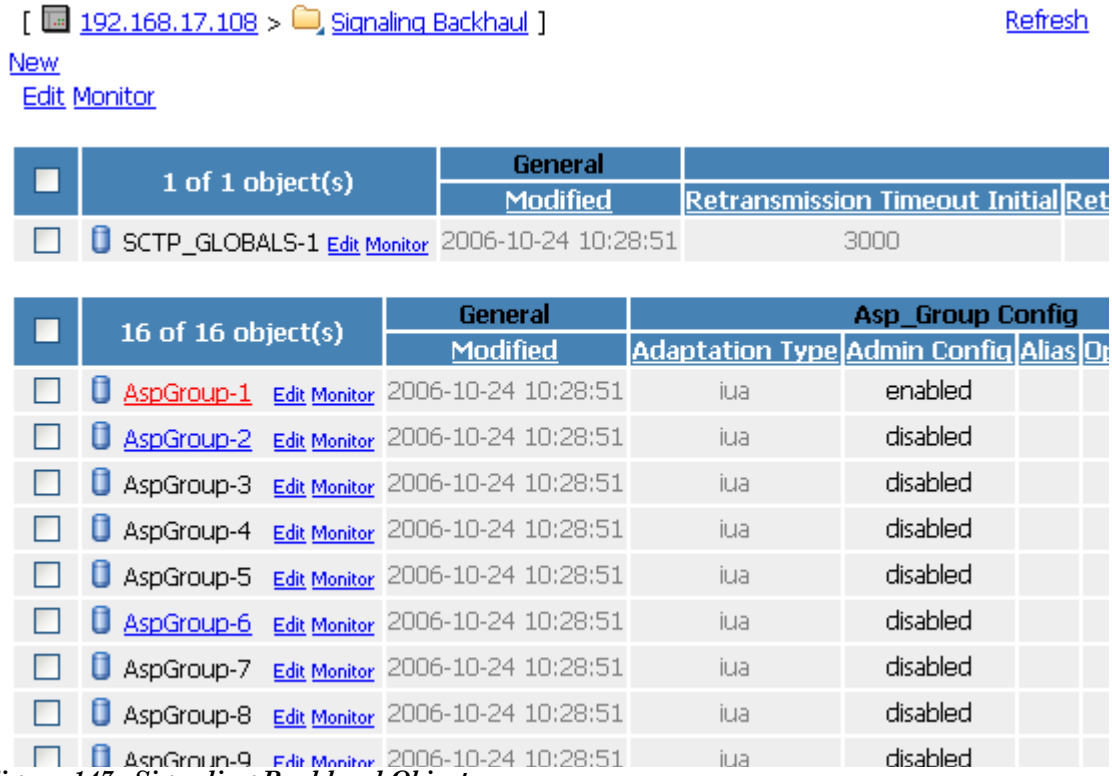


Figure 147. Signaling Backhaul Objects

2. Select **Monitor** to the right of the **SCTP_Globals-1** link to display the corresponding information in the information pane, as shown in Figure 149.

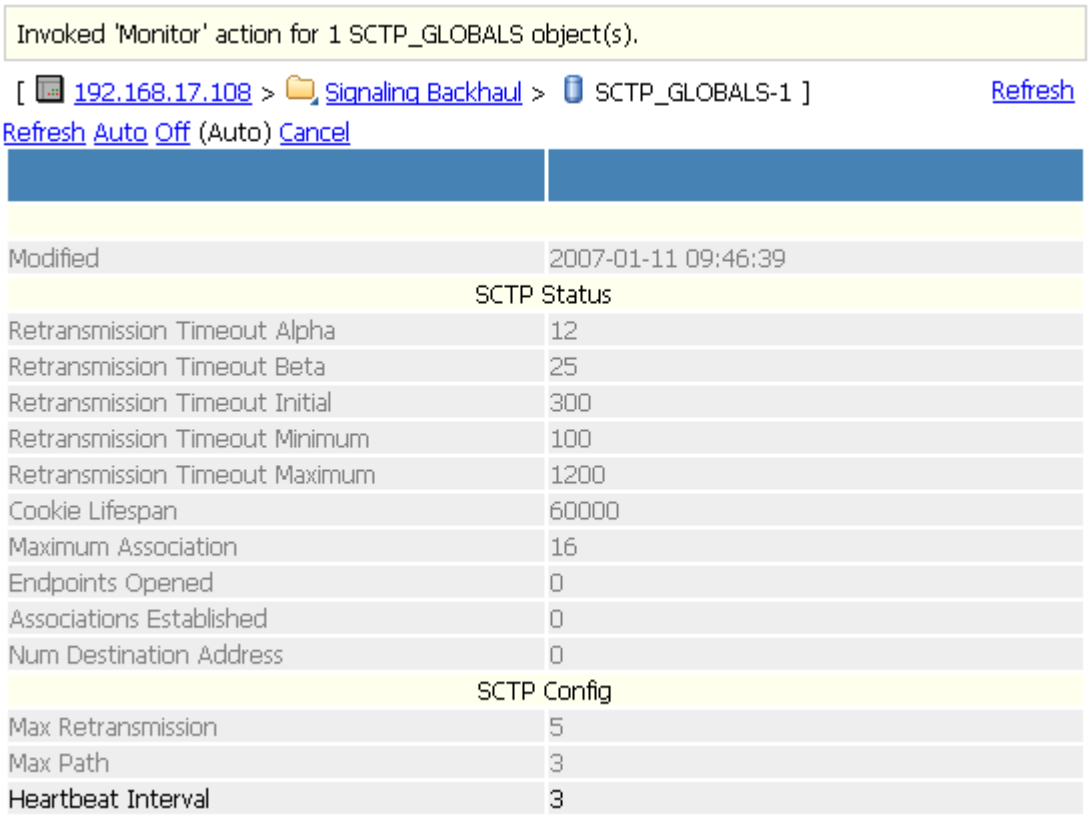


Figure 148. SCTP Status

Retransmission Timeout Alpha

The value of alpha used in the calculation of RTO multiplied by one hundred.

Retransmission Timeout Beta

The value of beta used in the calculation of RTO multiplied by one hundred.

Retransmission Timeout Initial

The initial RTO set before adjustment.

Retransmission Timeout Mininum

The minimum value of RTO after adjustment.

Retransmission Timeout Maximum

The maximum value of RTO after adjustment.

Cookie Lifespan

The lifespan of a valid cookie since its creation.

Maximum Association

The maximum number of associations for the gateway.

Endpoints Opened

The number of ASPs opened.

Associations Established

the number of associations established.

Num Destination Address

The number of destination addresses in use.

Max Retransmission

The number of times that an SCTP message will be retransmitted for an association if no response is received, regardless of the transport address.

Max Path

The number of times that an SCTP message will be transmitted to a particular transport address. Note than an association may have multiple transport addresses per association.

SCTP Association Stats	
Data Bytes Tx	0
Chunks Tx	0
Init Chunks Tx	0
Init Ack Chunks Tx	0
Cookie Chunks Tx	0
Cookie Ack Chunks Tx	0
Data Chunks Tx	0
Sack Chunks Tx	0
Heart Beat Chunks Tx	0
Heart Beat Ack Chunks Tx	0
Abort Chunks Tx	0
Shutdown Chunks Tx	0
Shutdown Ack Chunks Tx	0
Shutdown Compl Chunks Tx	0
Error Chunks Tx	0
Data Bytes Rx	0
Chunks Rx	0
Init Chunks Rx	0
Init Ack Chunks Rx	0
Cookie Chunks Rx	0
Cookie Ack Chunks Rx	0
Data Chunks Rx	0
Sack Chunks Rx	0
Heart Beat Chunks Rx	0
Heart Beat Ack Chunks Rx	0
Abort Chunks Rx	0
Shutdown Chunks Rx	0
Shutdown Ack Chunks Rx	0
Shutdown Compl Chunks Rx	0
Error Chunks Rx	0
DNSQuery Tx	0
DNSResp Rx	0
Clear Stats	noop

Figure 149. SCTP Association Statistics (cropped)

Data Bytes Tx

The total number of data bytes transmitted.

Chunks Tx

The total number of SCTP chunks transmitted.

Init Chunks Tx

The total number of SCTP INIT chunks transmitted.

Init Ack Chunks Tx

The total number of SCTP INIT ACK chunks transmitted.

Cookie Chunks Tx

The total number of SCTP Cookie chunks transmitted.

Cookie Ack Chunks Tx

The total number of SCTP Cookie ACK chunks transmitted.

Data Chunks Tx

The total number of SCTP Data chunks transmitted.

Sack Chunks Tx

The total number of SCTP SACK chunks transmitted.

Heart Beat Chunks Tx

The total number of SCTP Heart Beat chunks transmitted.

Heart Beat Ack Chunks Tx

The total number of SCTP Heart Beat ACK chunks transmitted.

Abort Chunks Tx

The total number of SCTP Abort chunks transmitted.

Shutdown Chunks Tx

The total number of SCTP Shutdown chunks transmitted.

Shutdown Ack Chunks Tx

The total number of SCTP Shutdown ACK chunks transmitted.

Shutdown Compl Chunks Tx

The total number of SCTP Shutdown Complete chunks transmitted.

Error Chunks Tx

The total number of SCTP Error chunks transmitted.

Data Bytes Rx

The total number of data bytes received.

Chunks Rx

The total number of SCTP chunks received.

Init Chunks Rx

The total number of SCTP INIT chunks received.

Init Ack Chunks Rx

The total number of SCTP INIT ACK chunks received.

Cookie Chunks Rx

The total number of SCTP Cookie chunks received.

Cookie Ack Chunks Rx

The total number of SCTP Cookie ACK chunks received.

Data Chunks Rx

The total number of SCTP Data chunks received.

Sack Chunks Rx

The total number of SCTP SACK chunks received.

Heart Beat Chunks Rx

The total number of SCTP Heart Beat chunks received.

Heart Beat Ack Chunks Rx

The total number of SCTP Heart Beat ACK chunks received.

Abort Chunks Rx

The total number of SCTP Abort chunks received.

Shutdown Chunks Rx

The total number of SCTP Shutdown chunks received.

Shutdown Ack Chunks Rx

The total number of SCTP Shutdown ACK chunks received.

Shutdown Compl Chunks Rx

The total number of SCTP Shutdown Complete chunks received.

Error Chunks Rx

The total number of SCTP Error chunks received.

DNSQuery Tx

The total number of SCTP association DNS queries transmitted.

DNSResp Rx

The total number of SCTP association DNS responses received.

ASPGroup Status

The following section discusses how to monitor ASPGroup status and provides brief descriptions of each parameter or statistic.

To view ASPGroup options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** > **AspGroup-n** to display the corresponding information in the information pane, as shown in Figure 150.

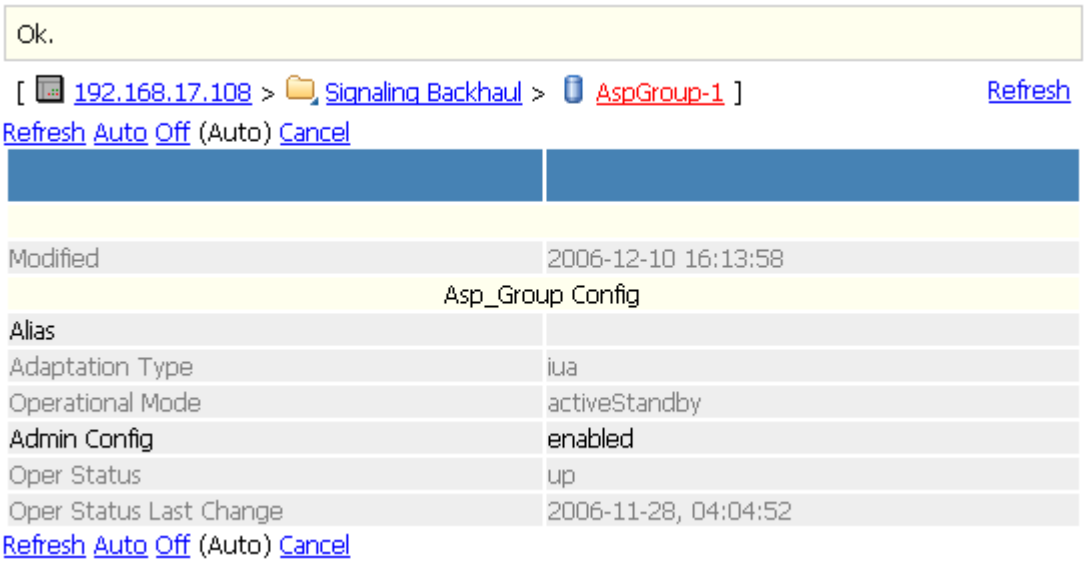


Figure 150. AspGroup Statistics

Adaptation Type

In this release, only IUA is supported.

Operational Mode

In activeStandby mode, only one ASP within the ASP group can be active at a time, while the others are in standby or non-operational (such as ASP_DOWN). In this release, this is the only supported Operational Mode.

Oper Status

The current operational status of the nodal interworking function (NIF). The possible states are: up, down (corresponding to enabled or disabled Admin Config) or missingBackhauls, if the Admin Config is enabled but no backhaul trunks have been assigned to this ASP Group.

Oper Status Last Change

The date and time of the last change to the operational status.

ASP Status

The following section discusses how to monitor ASP status and provides brief descriptions of each parameter or statistic.

To view ASP options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** > **AspGroup-n** to display the corresponding AspGroup objects in the information pane, as shown in Figure 151.

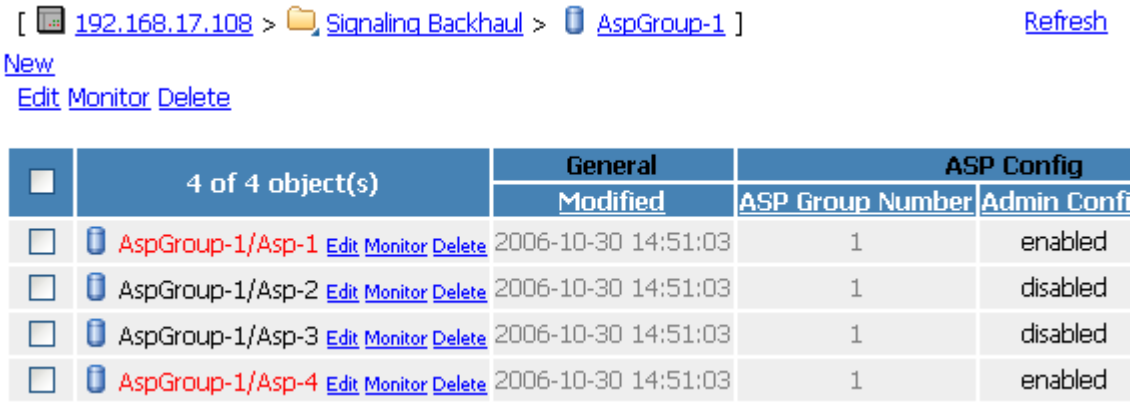


Figure 151. AspGroup Objects

2. Select **Monitor** to the right of the **Asp-1** to display the corresponding information in the information pane, as shown in Figure 152.

ASP Config	
Index	1
Alias	999
Admin Config	enabled
ASP Group Number	1
ASP Status	
ASP Oper Status	aspDown
Oper Status Last Change	n/a
Active Interface Count	0
Retransmission Timeout Current	0
SCTP Config	
Local Port	123
Remote Address	1.1.1.1
Remote Port	111
SCTP Status	
Oper Status	closed
Oper Status Last Change	n/a
Checksum Algorithm	crc-32
Remote Primary Addr	0.0.0.0
Remote Host Name	
In Streams	168
Out Streams	168
Peer Remote Port	0

Figure 152. ASP / SCTP Status

ASP Oper Status

The current operational status of the ASP that the gateway maintains through received maintenance messages.

Oper Status Last Change

The time of the last change to the operational status of the ASP.

Active Interface Count

The current active backhaul interface count.

Retransmission Timeout Current

This is the current retransmission timeout (RTO) value.

Local Port

This is the port number on which the gateway receives SCTP messages; for IUA, this is always 9900.

Oper Status

The operational status of the SCTP association that the gateway maintains through the exchanged SCTP messages.

Oper Status Last Change

The timestamp marking the last change of the operational status of the SCTP association.

Checksum Algorithm

The algorithm to compute the 32-bit checksum for the SCTP packet.

Remote Primary Addr

The primary address of the remote node with which the SCTP association is established.

Remote Host Name

The host name of the remote node with which the SCTP association is established.

In Streams

The maximum number of inbound streams allowed in the SCTP association.

Out Streams

The maximum number of outbound streams allowed in the SCTP association.

Peer Remote Port

The SCTP port number from which the ASP sends.

ASP Stats	
Pdu Tx	0
Pdu Byte Tx	0
Qptm Msg Tx	0
Aspsm Msg Tx	0
Asptm Msg Tx	0
Mgmt Msg Tx	0
Maup Msg Tx	0
Pdu Rx	0
Pdu Byte Rx	0
Qptm Msg Rx	0
Aspsm Msg Rx	0
Asptm Msg Rx	0
Mgmt Msg Rx	0
Maup Msg Rx	0
Clear Stats	noop

Figure 153. ASP Statistics (continued)

Pdu Tx

The total number of Protocol Data Units transmitted.

Pdu Byte Tx

The total byte count of the PDUs transmitted.

Qptm Msg Tx

The total number of QPTM messages transmitted.

Aspsm Msg Tx

The total number of ASPSM messages transmitted.

Asptm Msg Tx

The total number of ASPTM messages transmitted.

Mgmt Msg Tx

The total number of MGMT messages transmitted.

Maup Msg Tx

The total number of MAUP messages transmitted.

Pdu Rx

The total number of Protocol Data Units received.

Pdu Byte Rx

The total byte count of the PDUs received.

Qptm Msg Rx

The total number of QPTM messages received.

Aspsm Msg Rx

The total number of ASPSM messages received.

Asptm Msg Rx

The total number of ASPTM messages received.

Mgmt Msg Rx

The total number of MGMT messages received.

Maup Msg Rx

The total number of MAUP messages received.

Backhaul Trunk Status

The following section discusses how to monitor Backhaul Trunk status and provides brief descriptions of each parameter or statistic.

To view Backhaul trunk options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Signaling Backhaul** > **AspGroup-n** to display the corresponding AspGroup objects in the information pane, as shown in Figure 154.

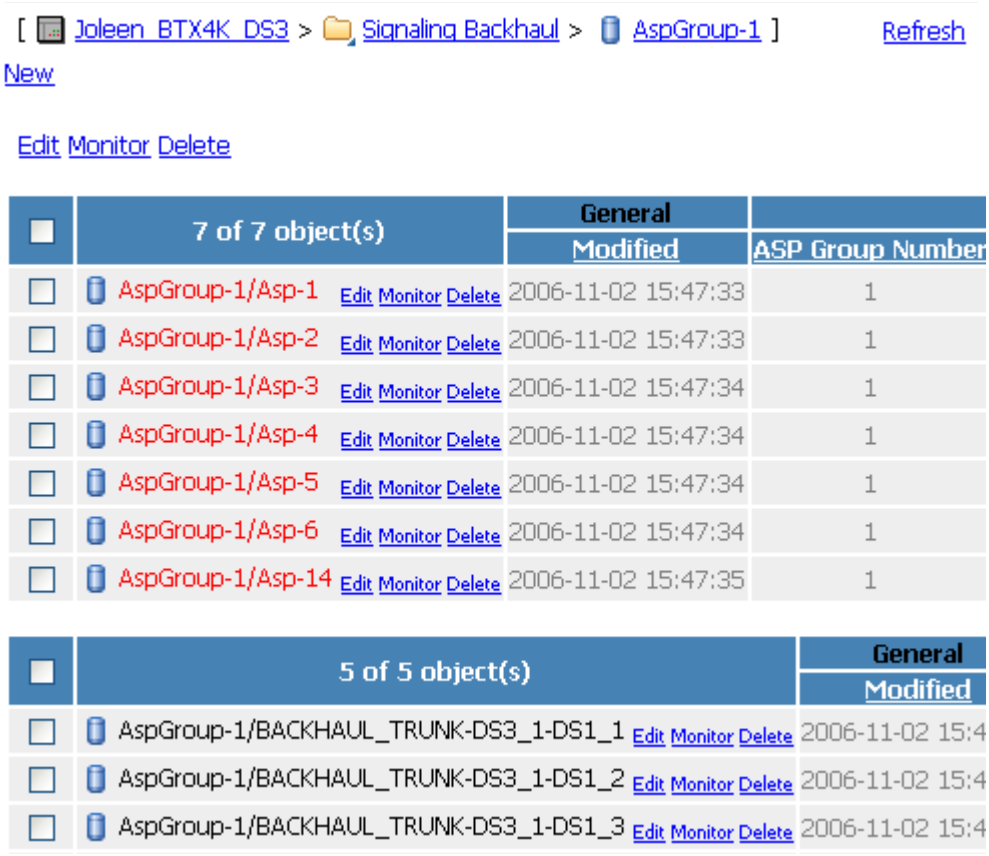

[Joleen_BTX4K_DS3 > Signaling Backhaul > AspGroup-1] Refresh
New
Edit Monitor Delete
7 of 7 object(s)
General
Modified
ASP Group Number
AspGroup-1/Asp-1 Edit Monitor Delete 2006-11-02 15:47:33 1
AspGroup-1/Asp-2 Edit Monitor Delete 2006-11-02 15:47:33 1
AspGroup-1/Asp-3 Edit Monitor Delete 2006-11-02 15:47:34 1
AspGroup-1/Asp-4 Edit Monitor Delete 2006-11-02 15:47:34 1
AspGroup-1/Asp-5 Edit Monitor Delete 2006-11-02 15:47:34 1
AspGroup-1/Asp-6 Edit Monitor Delete 2006-11-02 15:47:34 1
AspGroup-1/Asp-14 Edit Monitor Delete 2006-11-02 15:47:35 1
5 of 5 object(s)
General
Modified
AspGroup-1/BACKHAUL_TRUNK-DS3_1-DS1_1 Edit Monitor Delete 2006-11-02 15:4
AspGroup-1/BACKHAUL_TRUNK-DS3_1-DS1_2 Edit Monitor Delete 2006-11-02 15:4
AspGroup-1/BACKHAUL_TRUNK-DS3_1-DS1_3 Edit Monitor Delete 2006-11-02 15:4

Figure 154. AspGroup Objects

2. Select **Monitor** to the right of the **AspGroup-1/BACKHAUL_TRUNK_DS3_1-DS1_1** to display the corresponding information in the information pane, as shown in Figure 155.

Modified	2006-11-02 17:00:49
TRUNK Config	
Adaptation Type	iua
IUATimeslot	24
Interface ID	1
Asp Group Number	1
TRUNK Status	
Oper Status	down
Oper Status Last Change	2006-08-30, 19:54:58
Add Delete Oper Status	none
Add Delete Oper Status Last Change	2006-08-24, 12:47:11
Lapd Config	
Isdn Switch Type	ni2
Isdn Protocol Type	network
TRUNK Stats	
lapd IFrame Tx	0
lapd SFrame Tx	0
lapd UFrame Tx	0
lapd IFrame Rx	0
lapd SFrame Rx	0
lapd UFrame Rx	0
lapd Invalid Frame Rx	0
lapd Sabme Error	0
lapd Frmr Error	0
lapd Clear Stats	noop

Figure 155. Backhaul Trunk Parameters and Statistics

Oper Status

- **up** - The nodal interworking function is up.
- **down** - The configuration is otherwise good but the nodal interworking function is down.
- **insufficientResources** - The configuration is otherwise good but there are not enough physical resources to support the configuration.
- **badTimeslot** - The configured timeslot is invalid (i.e., -1 for E1 or -1, 0, 25..31 for T1).

Oper Status Last Change

The date and time of the last change to the operational status.

Add Delete Oper Status

This provides information on the success or failure (or none) of the last trunk added or deleted to the ASP Group.

Add Delete Oper Status Last Change

The last time the value of Add Delete Oper Status changed.

lapd IFrame Tx

The total number of information frames transmitted.

lapd SFrame Tx

The total number of supervisory frames transmitted.

lapd UFrame Tx

The total number of unnumbered frames transmitted.

lapd IFrame Rx

The total number of information frames received.

lapd SFrame Rx

The total number of supervisory frames received.

lapd UFrame Rx

The total number of unnumbered frames received.

lapd Invalid Frame Rx

The total number of invalid frames received.

lapd Sabme Error

The total number of SABME state errors.

lapd Frmr Error

The total number of FRMR state errors.

System Globals Status

The following section discusses how to monitor System Globals status and provides brief descriptions of each parameter or statistic.

To view System Globals options and statistics:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/system** to view the table shown in Figure 156.

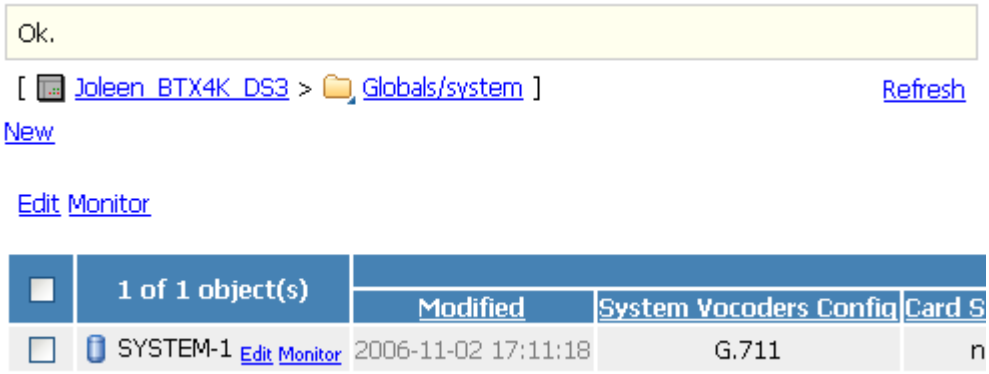


Figure 156. System Global Objects

2. Select **Monitor** to the right of **System-1** to display the corresponding information in the information pane, as shown in Figure 157.

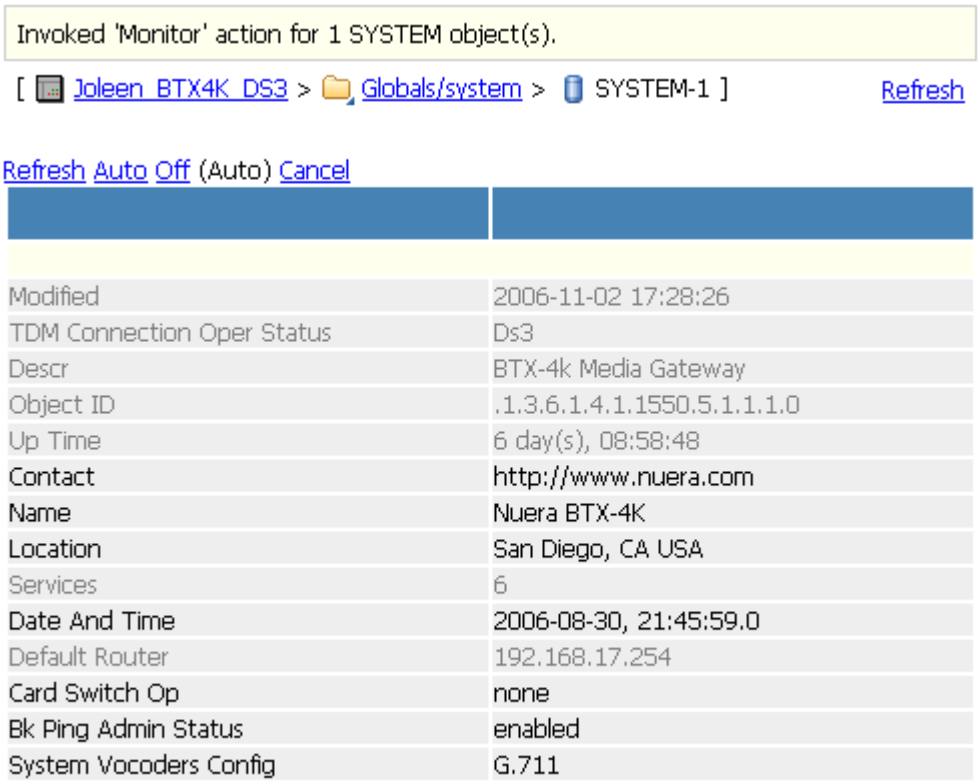

Invoked 'Monitor' action for 1 SYSTEM object(s).
[Joleen_BTX4K_DS3 > Globals/system > SYSTEM-1]
Refresh
Refresh Auto Off (Auto) Cancel
Modified 2006-11-02 17:28:26
TDM Connection Oper Status Ds3
Descr BTX-4k Media Gateway
Object ID .1.3.6.1.4.1.1550.5.1.1.1.0
Up Time 6 day(s), 08:58:48
Contact http://www.nuera.com
Name Nuera BTX-4K
Location San Diego, CA USA
Services 6
Date And Time 2006-08-30, 21:45:59.0
Default Router 192.168.17.254
Card Switch Op none
Bk Ping Admin Status enabled
System Vocoders Config G.711

Figure 157. System Globals Parameters and Statistics

TDM Connection Oper Status

This displays the current TDM interface for the gateway, which is based on the VPM type and TDM configuration performed at the console port.

Descr

A textual description of the entity.

Object ID

The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor `Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its `Fred Router'.

Up Time

The time since the network management portion of the system was last re-initialized.

Services

Consistent with the SNMP description of a system, this value indiates the set of services this system offers. The value 6 indicates this system offers Internet services.

Default Router

This agent's default router.

5

MANAGING THE GATEWAY

This chapter describes how to monitor the health of the BTX-4K gateway, upgrade the gateway, and use the gateway's debugging features.

Using Syslog

The BTX-4K provides a debug trace capability using the Syslog protocol. This protocol provides a transport to allow the BTX-4K to send event messages across IP networks to a collector known as a Syslog server. The Syslog protocol uses the standard UDP port 514. There are many off-the-shelf Syslog server programs that can be installed and run on a PC.

The source IP address of the Syslog message is the Background Control IP address of the sourcing VPM. This IP address is unique to each VPM, allowing the differentiation of messages from the active and standby VPMs.

To set the destination IP address for gateway Syslog messages:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/Syslog** as shown in Figure 158.

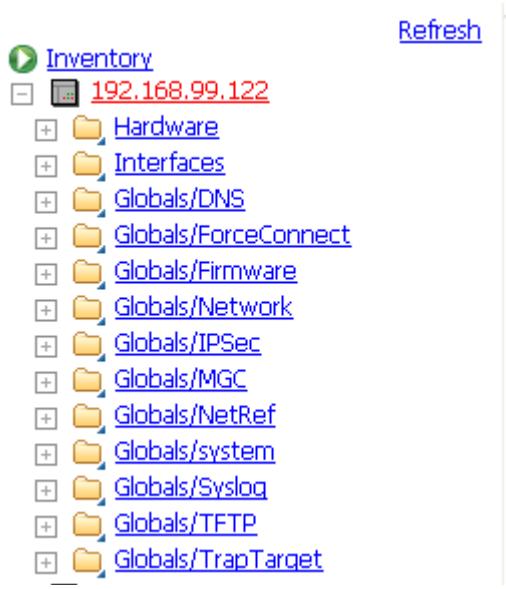


Figure 158. Navigating to Syslog Table

2. As shown in Figure 159, select **Edit** to the right of the **Syslog Globals-1** link.

Figure 159. Syslog Table

3. After selecting **Edit**, the syslog configuration screen shown in Figure 160 will

appear.

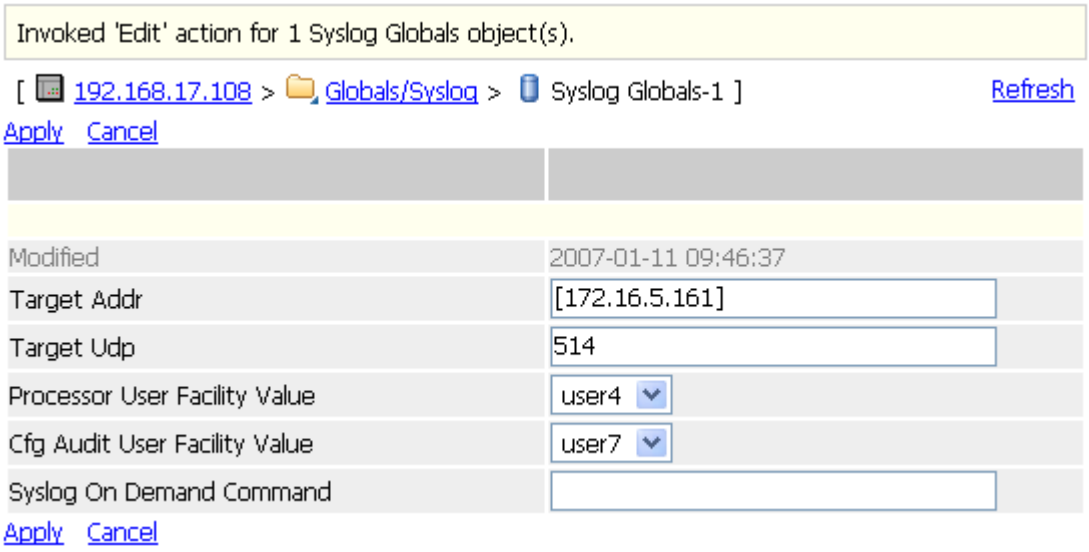
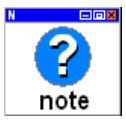


Figure 160. Syslog Configuration Parameters

4. Configure **Target Addr**. This is the IP address of the PC running the syslog software.
5. Configure **Target UDP**. This is the target UDP port for debug messages, typically 514 (default syslog UDP port).
6. Select the desired **Processor User Facility Value**. This parameter identifies the Syslog facility (i.e. group) assigned to BTX-4K Debug messages. It may be configured from user0 (local user0) to user7 (local user7). It may be configured the same as Cfg Audit User Facility Value but the default is different.
7. Select the desired **Cfg Audit User Facility Value**. This parameter identifies the Syslog facility (i.e. group) assigned to BTX-4K Configuration Audit messages. It may be configured fromuser0 (local user0) to user7 (local user7). It may be configured the same as Processor User Facility Value but the default is different.

Some Syslog servers use the Facility Value to store Syslog messages to different files. If you cannot locate syslog messages, check your Syslog server configuration.

8. Enter the **Syslog On Demand Command**. Typically the **Syslog On Demand Command** is used under the direction of Nuera TAC to provide detailed troubleshooting and diagnostic data.



A result of sending the syslog on demand command to the BTX-4K is a syslog message that comes out to the same destination as the unsolicited debug class syslogs

9. Click **Apply**.

Configuring Debug classes

Syslog debug messages are divided into classes. Each class is independent and contains messages related to a particular functional module in the system. The setting of one class has no effect on any other class. All classes can be turned on, at different levels, at the same time. Selecting (or deselecting) classes allows you to customize the scope of the debug trace. These classes are divided into three main functional groups:

- CCP debug class - relates to items associated with the VPM, such as configuration, system, TDM, and security tasks.
- DSP debug class - relates to TGCP and voice processing. Some DSP syslog classes can be further filtered to specific DS3, DS1, or DS0s by using an index (called the ifIndex).
- NP debug class - relates to IP packet processing

Turning on every debug class to its highest level may cause congestion on your control port interface which can delay important TGCP and SNMP messages

To configure the debug class:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/Syslog**, as shown in Figure 161.

Figure 161. Navigation to Syslog Table

2. Select the **Edit** link next to the debug class you want to configure, as shown in Figure 162. For brief definitions of the debug classes see "Syslog Debug Classes" on page 211.

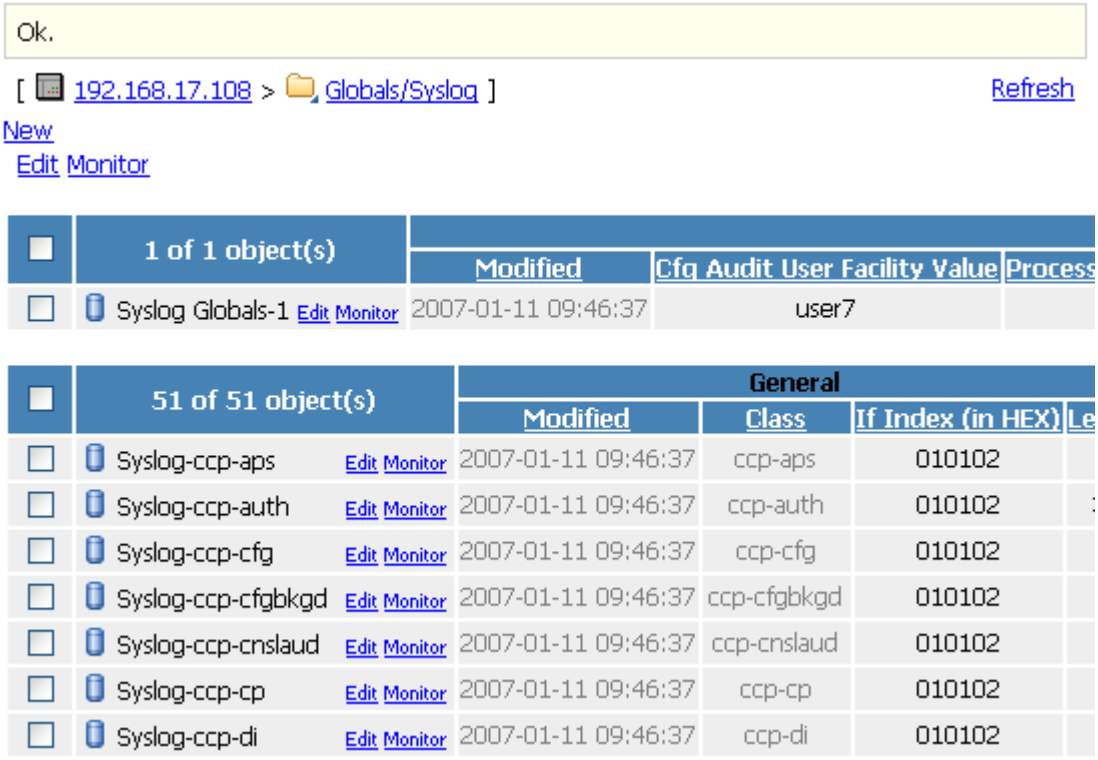


Figure 162. Debug Class Table

3. Select **Edit** to the right of the debug class you want to configure, as shown in Figure 162. For brief definitions of the debug classes see "Syslog Debug Classes" on page 211.

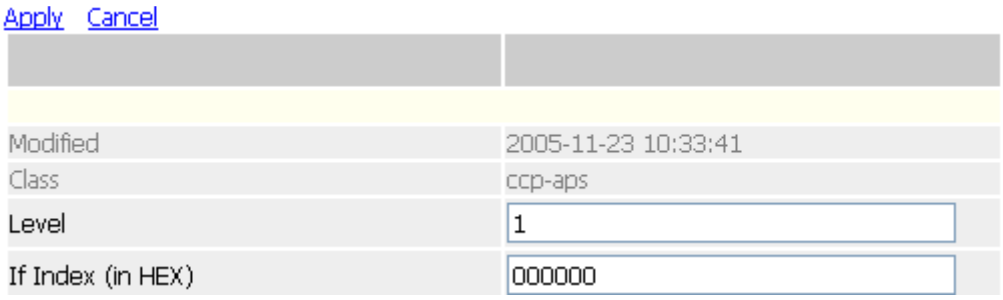


Figure 163. Debug Class Configuration

4. Configure **Level**. This is the debug level for this debug class. A value of zero effectively disables debug for this class. The higher the number, the more debug information is available. The default level for all classes is Level **1**. Configurable levels are:
   - **Level 0** – Disabled, no syslog output for the given class.

- **Level 1** – Critical/Error Condition. This is the default setting on the VPM
- **Level 2** – Call/Operational Flow. This is informational as to the general flow of the software.
- **Level 3** – Function Trace/Informational. This is a detailed trace at the function level, used mostly for unit testing.
- **Level 4** – Verbose (DSP only).

5. Configure **ifIndex**. The Interface Index, or **ifIndex**, is a filter for the debug class, when applicable. In addition to using levels, some of the DSP syslog classes can be further filtered to specific DS3, OC-3, DS1, STM-1, E1 or DS0s by using an **ifIndex** specific to the endpoint (or group of endpoints). This option is not available to CCP and NP classes.

   A value of zero enables debugging for all interface objects for this class. A non-zero value enables debugging for that particular interface object only. It is not applicable to CCP and NP classes.

   DS3 Only

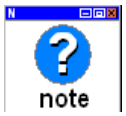
   Enter this value as a decimal representation of a hexadecimal number, xx/yy/zz, where:

   - xx is the DS3 number
   - yy is the DS1 number. (A value of 00 means all DS1s.)
   - zz is the DS0 number. (A value of 00 means all DS0s.)

   For example:

   65536 = 01/00/00 or 10000 in hexadecimal. This includes all DS1s and all DS0s on DS3 number 1.

   65793 = 01/01/01 or 10101 in hexadecimal. This includes DS0 number 1 on DS1 number 1 on DS3 number 1.

   The Index Value under DS0 General Statistics is calculated this way and can be used as a quick reference for individual DS0s.

   OC-3 Only

   Enter this value as a decimal representation of a hexadecimal number, vv/xx/yy/zz, where:

- vv is the OC-3 number
- xx is the STS Path number (0, 1, 2, or 3, in groups of 28 T1s. A value of 00 means all STS-1 paths.)
- yy is the DS1 number. (A value of 00 means all DS1s.)
- zz is the DS0 number. (A value of 00 means all DS0s.)

For example:

16777216 = 01/00/00/00 or 1000000 in Hex. This includes all DS0s on all STS-1 paths on OC-3 number 1.

16843009 = 01/01/01/01 or 1010101 in Hex. This includes DS0 number 1 on DS1 number 1 on STS-1 path number 1 on OC-3 number 1.

The Index Value under DS0 General Statistics is calculated this way and can be used as a quick reference for individual DS0s.

STM-1 Only

Enter this value as a decimal representation of a hexadecimal number, vv/xx/yy/zz, where:

- vv is the STM-1 number
- xx is the VC4 Path number (always 01)
- yy is the E1 number. (A value of 00 means all E1s.)
- zz is the DS0 number. (A value of 00 means all DS0s.)

For example:

16777216 = 01/00/00/00 or 1000000 in Hex. This includes all DS0s on all DS1s on all VC-12 paths on STM-1 number 1.

16843009 = 01/01/01/01 or 1010101 in Hex. This includes DS0 number 1 on DS1 number 1 on VC-12 path number 1 on STM-1 number 1.

The Index Value under DS0 General Statistics is calculated this way and can be used as a quick reference for individual DS0s.

6. Click **Apply**.

Upgrading the Firmware

Firmware updates are necessary when Nuera releases new gateway code for upgrade. Code is delivered as a ***.zip** file. The new gateway code will be delivered to you through the Nuera web site or on a CD. Please refer to the *NetConductor User Manua*l for details on loading code to a gateway.

You can download the code from the NetConductor server to the BTX-4K VPMs in the background while the VPMs are in operation without affecting calls. The code download occurs across the background control IP addresses. Verify that these have been properly assigned during initial system configuration to ensure successful code downloads.

You can also configure the NetConductor server to download firmware code to the BTX-4K via TFTP within a secured IPSec tunnel. In order to use secure firmware transfers the raccoon process must be setup on the NetConductor Server (refer to the *NetConductor User's Manual* for information on configuring this process). In addition, secure TFTP must be selected in the Firmware configuration screen (see below).

During firmware upgrade, or when installing a spare VPM with a different firmware version, the standby VPM may indicate it has a fault (red LED). This is a transitory state that indicates that the code on the two VPMs is not the same, but is not service affecting and in no way prevents the firmware upgrade from proceeding. Once the firmware upgrade is complete the fault indication will go away.

To upgrade the firmware:

1. Expand the hierarchy by selecting **Inventory** > [NE] > **Globals/Firmware**. The

information pane will display the firmware table shown in Figure 164.

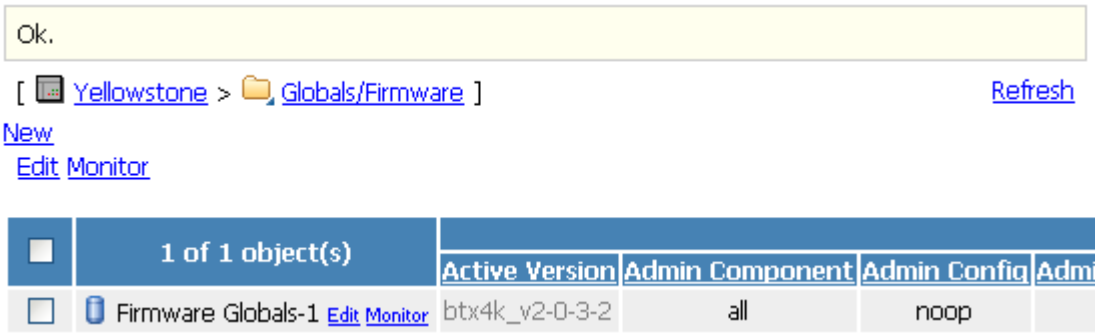


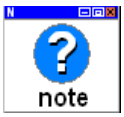
Figure 164. Firmware Table

2. Click the **Edit** link to display the Firmware Globals configuration screen shown in Figure 165.

Figure 165. Firmware Configuration

3. Select the **Admin Version**. This is the version to which you want to upgrade. In the drop-down menu in this field all gateway code versions in the firmware directory on the NetConductor server are listed for the particular NE type that is currently configured for the gateway. If you do not see the code version you want, you may need to change the NE type of your gateway.
4. Configure **Admin Component** to **all**.
5. The **Admin Config** parameter indicates how the firmware is processed by the BTX-4K. **Admin Config** may be set to the following values:

- **updateAndActivateAll** - This option updates and activates the new code on both VPMs. To start the process, code is downloaded to the background code banks on the active and standby VPM cards. The standby card will be reset to activate the new code. Once the standby card comes up with the new code, the active card will be reset to activate the code. The standby card (running the new code) will then take over as active. This process will take several minutes to complete.



This is the recommended command/procedure for performing firmware upgrades.

- updateAndActivateStandby - This option updates and activates the standby VPM card. Two typical uses for this command are:
  - When a VPM is replaced with a spare operating with an older version of code. The active card has the latest version leaving only the standby to be upgraded and activated.
  - If there was an IP problem during the **updateAndActivateAll** upgrade that prevented the standby card from upgrading.
- **updateStandby** - This option downloads the code to the background code bank on the standby VPM card. Two typical uses for this command are:
  - To allow verification of a successful code download prior to resetting and activating the standby VPM card.
  - If the person responsible for downloading the card is different than the person who controls resets on the VPM card. For example, the code could be downloaded ahead of time with the activation occurring later during a maintenance window.
- **activateStandby** - This option activates the standby VPM. This command is most often used in conjunction with the **updateStandby** command.
- **forceOver** - This command forces the standby VPM to become the active VPM.

6. The **Active Version** displays the current version of the code and **Backup Version** displays the backup version.
7. Configure **Secure TFTP**. When **enabled**, the firmware transfer from the NetConductor to the gateway will be within an IPSec tunnel, provided that the raccoon process is properly configured on the NetConductor server.
8. Select **Apply**.

The **Oper Status** parameter will provide updates on the progress of the firmware upgrade and will indicate when the process is complete.

The Alarm pane will report any errors encountered during the firmware upgrade process.

Upgrading Capacity and Vocoder Capability

To upgrade the Capacity or Vocoder Capability of the BTX-4K, contact your Nuera representative with the following information:

- current capacity license
- current vocoder license
- serial numbers for both VPMs

You can locate this information by selecting **Tasks** from the Link pane at the top of the NetConductor window. In the navigation pane on the left, select the appropriate Network Element, then **License** to display this information as shown in Figure 166.

Ok.

NE Name
192.168.99.122/161

IP

	Default Gateway/Router	IP address	Subnet Mask
Floating IP-control	192.168.99.254	192.168.99.122	255.255.255.0
Floating IP-media	192.168.99.254	192.168.99.222	255.255.255.0

Slot-1

	Current Capacity Licensed	Current Vocoder Licensed	Number of DSP SIMMs	Serial Num
Vpm-1	1302	g711 + g729a	11	350400162

Slot-2

	Current Capacity Licensed	Current Vocoder Licensed	Number of DSP SIMMs	Serial Num
Vpm-2	1302	g711 + g729a	11	270405525

Figure 166. License Information pane

After processing your upgrade request, Nuera will send you upgrade installation instructions, upgrade license files, and additional DSP modules. You are ready to begin the upgrade procedure.

Maintenance Procedures

The following sections detail paths and procedures necessary to perform routine maintenance on your system.

Forcing a Switchover

If necessary, you can make your backup VPM the active VPM by forcing a switchover.

To force a switchover:

Expand the hierarchy in the Navigation pane by selecting **Inventory** > [NE] > **System**. The Information pane will change to display the contents of Figure 167.

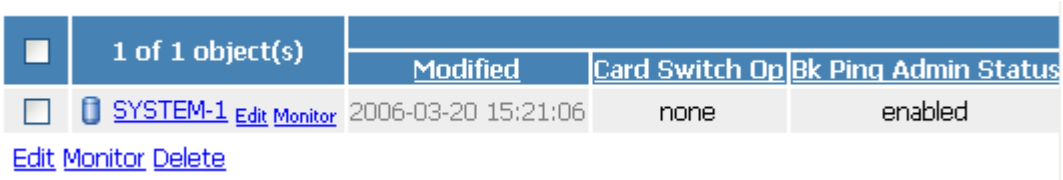


Figure 167. System Table (Forcing a Switchover)

9. Select **Edit** to display the **System** configuration screen shown in Figure 168.

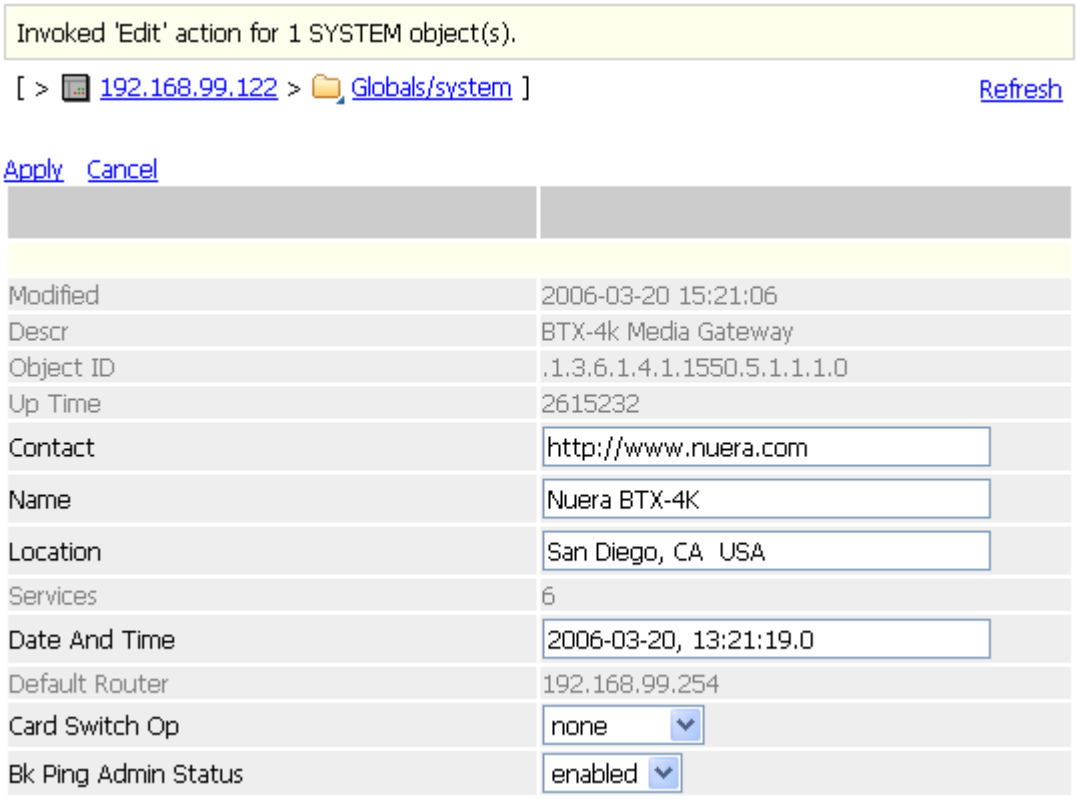
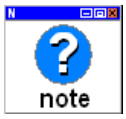


Figure 168. System Configuration Screen (Forcing a Switchover)

10. From the **Card Switch Op** drop-down box, choose **forceOver**.



If the standby card is not in the Standby-Protect state, the forceOver will not occur. In other words, the system will not forceOver if the other card is not prepared to take over.

11. Click **Apply**.

The BTX-4K performs switchovers transparently. Media and management functions will not be interrupted.

Version Information

Follow the procedures below to determine the current gateway software versions.

Firmware Information

To obtain information about the software running on the gateway, expand the hierarchy by selecting **Inventory** [NE] > **Globals/Firmware**. The current firmware version for this NE, as shown in the Information pane in Figure 169, is **btx4k_v2-0-1-4**.

Refresh Auto Off (Auto) Cancel

Modified	2005-09-01 12:01:54
Admin Config	noop
Backup Version	btx4k_v2-0-1-4
Oper Status	idle
Active Version	btx4k_v2-0-1-4
Admin Version	none
Admin Component	

Figure 169. Globals/Firmware (Current Firmware Version)

6

TROUBLESHOOTING

This chapter highlights possible solutions to a number of common difficulties.

Connection Issues

Verify your connections. Verify that connections exist from the 100 BaseT and GigE Ethernet ports on the BTX-4K to the router(s) or switch(es). Verify ports are online, down to the DS1/E1 level.

IP Address Conflicts

All six IP addresses associated with the BTX-4K gateway must be unique to your network. The VPM will not come up if it detects a conflict on one of its Ethernet interfaces. The craft port will be available to change the IP address if necessary.

License Upgrade Issues

Symptoms

Authorization file is initiated from a PC but cannot see new license at the gateway.

Possible Causes

- PC not in TFTP access list.
- Connection issue between NetConductor and Gateway, including a firewall block for TFTP packets or Background Control IP addresses.
- Background Control IP addresses not properly configured during initial system configuration.

- Excessive congestion in IP Network causes download to timeout.

Solutions

- Add PC IP address the TFTP access list.
- Configure firewall to allow TFTP packets on UDP ports 69 and 1500 and to allow traffic to/from the Background Control IP addresses.
- Verify that the Background Control IP addresses are unique and routable IP addresses. If not, you must reconfigure these addresses at the craft port of the active VPM. A service-affecting system reset will also be required.
- Resolve traffic congestion issues.

Firmware Upgrade Issues

Symptoms

Code upgrade is initiated at NetConductor but cannot see new code at the gateway.

Possible Causes

- Connection issue between NetConductor and Gateway, including a firewall block for TFTP packets or Background Control IP addresses.
- Background Control IP addresses not properly configured during initial system configuration.
- Excessive congestion in IP Network causes download to timeout.

Solutions

- Configure firewall to allow TFTP packets on UDP ports 69 and 1500 and to allow traffic to/from the Background Control IP addresses.
- Verify that the Background Control IP addresses are unique and routable IP addresses. If not, you must reconfigure these addresses at the craft port of the active VPM. A service-affecting system reset will also be required.
- Resolve traffic congestion issues.

MO/MT Channel Issues

Symptoms – Scenario 1

MO/MT spans are not coming up (in other words, the span is not in service).

Possible Causes

- Robbed-bit signalling has not been selected. MO/MT are MF Feature Group D trunks and Robbed-bit signalling should be selected for the DS1 that is running MO/MT signalling.

Solutions

- From the hierarchy in the NetConductor navigation pane, select **Inventory** > [NE] > **Interfaces** > **DS3-n**. Select **edit** next to the corresponding DS1 In the displayed dialog box, set **SignalMode** to **robbed bit**.

Symptoms – Scenario 2

MO or MT channels do not make outbound calls.

Possible Causes

- MO trunk: The operator has disabled the channel(s) by reverse make busy on the channel on the MO trunk.
- MT trunk: Configuration error. MT channels are for operator-assisted inbound calls or for busy line verification only. They are not meant for making outbound calls.

Solutions

- MO trunk: Contact the operator (OSS) to check if the channel(s) has been disabled.
- MT trunk: Contact the operator or move the MT spans/channels to the correct channel resource.

MG to MGC Communications

Symptoms – Scenario 1

Media Gateway (MG) messages are not being seen or responded to by the Media Gateway Controller (MGC). For example, RSIP/NTFYs from the media gateway (MG) are not being responded to by the MGC. CRCX/RQNTs from the MGC responded to by the MG but the MGC retransmits the same commands.

Possible Causes

- The IP of the MGC was entered incorrectly in the MGC target table.
- The domain name of MGC was entered incorrectly in MGC target table.
- The domain name of MGC was not entered correctly in the DNS.
- The MG domain name was not entered correctly in the MGC.

- The MG domain name was not entered correctly in the DNS.
- The DNS is not up.
- The UDP port for MGC is not correct.

Solutions

- Check the DNS. Verify all names and IPs of the MGCs and the MGs.
- Navigate NetConductor hierarchy: **Inventory** > [NE] > **Globals/MGC**. Verify names and UDP ports in the templates.
- Check that the IP address on the **DNS server-1** is correct in the NetConductor, under **Inventory** > [NE] > **Globals/DNS**, and in the MGC.
- In the NetConductor, under **Inventory** > [NE] > **Globals/DNS** > **DNS Resolver**, look at the MGC DNS resolved status. If **Status** is not **OK**, then verify the MGC name under **Inventory** > [NE] > **Globals/MGC** > **MGC Template**.
- Check that the domain name for the MG in the MGC matches that value stored in NetConductor under **Inventory** > [NE] > **Globals/MGC** > **MGC Globals-n**.

Symptoms – Scenario 2

MG does not see or respond to MGC commands. For example, RQNT/CRCX from MGC not being responded to by the MG. Or, the MGC is not in the list of valid MGCs for the affected DS3.

Possible Causes

- The UDP of the MG is different than 2427 in the MGC configuration. Refer to the previous Possible Causes.
- Call Pro is not enabled.

Solutions

- Verify that the setting for Call Pro Admin Config is enabled. For more information, see "Configuring DS1 and E1 Parameters" on page 68 for more information on setting this value.
- Refer to the previous Solutions.

Voice Issues

Symptoms – Scenario 1

You are experiencing one-way audio, severely distorted voice, or dropped calls.

Possible Causes

- The NetRef source is not set to BITS, DS1, OC-3, or STM-1, but is instead working from the local oscillator.
- Admin Config is not enabled.
- CMTS is sending a bandwidth setting to MTA that conflicts with network availability.

Solutions

- BTX-4K gateway receives external clock through the BITS interface, through the DS1 or through the OC-3 or STM-1 interface. In the NetConductor navigation pane, expand the hierarchy by selecting **Inventory >** [NE] **> Globals/NetRef** > **NetRef-1**. Click the **Edit** button for the first VPM card to configure the following:
  - Configure **Source.**
  - Enable **AdminConfig.**
- Repeat these steps for the second NetRef source.
- Check the CMTS configuration and ensure that what is available from the packet cable network is reflected in the NCS commands to the MTA.

Symptoms – Scenario 2

You are experiencing one-way audio, severely distorted voice, or dropped calls.

Possible Cause

- CIC values on the PSTN side and in the Class 5 CSSare different.

Solution

- Make sure that your Class 5 SSC has CIC values for the BTX-4K gateway trunks numbered the same way as the CIC values provided by the PSTN.

Symptoms - Scenario 3

There is only one-way audio.

Possible Cause

- The BTX-4K gateway's default router is behind the firewall and RTP packets cannot go through.

Solutions

- Verify that you have opened UDP ports in the router for voice packets coming from the gateway.
- The UDP range is from UDP_Base to UDP_Base + 4 * (number of channels used in the BTX-4K).

Fax/Modem Issues – Packet Loss

Symptoms

Fax/Modem transmission fails.

Possible Cause

- Network packet loss. Check the DS0 status for the packet loss.

Solution

- You need to find the source of the packet loss in the network.

Fax/Modem Issues – Clocking

Symptoms

Fax/Modem messages transmission fails.

Possible Causes

- The NetRef Source is set to none or the Admin Config is not enabled.

Solutions

- In the NetConductor navigation pane, expand the hierarchy by selecting **Inventory** > [NE] **> Globals/NetRef** > **NetRef-n**. Click the **Edit** button for the first VPM card to configure the following:
  - Configure **Source**.
  - Enable **Admin Config.**
- Repeat these steps for the second NetRef source.

100 BT Interface Issues

Symptoms

The SNMP request times out. Signalling messages have to be resent. There is a late, or no, ping response.

Possible Causes

- There is a network overload. Or the network is busy.
- The Debug Class levels are set too high and syslog messages are overloading the network.
- The 100 BaseT interfaces are connected to a device that is not configured as full duplex.

Solutions

- Rearrange the network to clean up the overloading.
- Check whether all routers and switches are set to full duplex since a 100 BaseT interface is full duplex.
- Check the cables and connections.
- Set Debug Class levels to 0 or 1.

A

SYSLOG DEBUG CLASSES

This appendix details the various debug classes. For information on how to configure debug classes see "Configuring Debug classes" on page 193.

CCP Classes

This section provides a short description of each CCP class. It gives you an idea of the kind of information that can selectively be generated on demand. You can turn these classes on or off as you need them

CCP_APS

This class contains information on the Automatic Protection Switch (APS) task for STM-1 and OC-3 interfaces.

CCP_AUTH

Information on upgrading and maintaining capacity and vocoder upgrades.

CCP_CFG

Information about the processing configuration in the system.

CCP_CFGBKGND

This class contains information about the configuration background task. It includes information on the low-level operations of updating configuration and routing this updated configuration to all registered tasks.

CCP_CNSLAUD

This turns audit messages due to configuration changes made at the console off (0) or on (1).

CCP_CP

This class provides information related to the Call Processing (CP) task. It provides information on the XCGP message routing.

CCP_DI

This class provides information related to the craft or Display (DI) task.

CCP_DNS

This class provides information about the DNS task. It reports status on the progress of DNS queries and the health of the DNS server.

CCP_Drivers

This class contains information about low level driver code related to Signaling Backhaul only.

CCP_DRVR

This class contains information about low level driver code related to netref, console ping and Ethernet packet transmission.

CCP_DSPAPI

This class provides information related to the DSP including DSP status, VPM-DSP messages, and DSP code downloading.

CCP_DSPPOLL

This class provides information on the DSP heartbeat poll. This status was separated from the CCP_DSPAPI because of its high rate repetitive nature.

CCP_EH

This class contains information related to the Event Handler (EV) task. This is the task that collects all the events and makes the decision about failover.

CCP_FATAL

This class provides information on fatal errors. All fatal error messages are sent regardless of the level set for this class.

CCP_FFS

This class contains information specific to the Flash File System (FFS) task. It reports low level information on the file access and storage init.

CCP_IDLE

This class contains information related to the idle task. It provides information on the percentage idle time in the system.

CCP_INIT

This class contains information about the initialization process. It deals with things such as booting from flash, hardware initialization, and task startup.

CCP_IP

This class provides information relating to IP address conflicts, ARP resolution, and internal IP function misuse.

CCP_IPSEC

Information on configuring and processing IPSec signaling packets.

CCP_IPTSK

This class contains information on the IP Task. It reports detailed information on the Ping functionality.

CCP_IUA

This class provides information about the IUA stack top level events.

CCP_IUANIF

This class provides information about NIF (Nodal Interface Function) layer events in the IUA stack.

CCP_LAPD

This class provides information about LAPD layer events from the IUA stack.

CCP_LED

This class provides information on LEDs; not currently used.

CCP_M2UA

For future use.

CCP_M2UANIF

For future use.

CCP_MTP2

For future use.

CCP_NPAPI

This class provides information about the Network Processor API task. It provides information related to the NP including NP status, VPM-NP messages, and NP code downloading.

CCP_NTP

Not currently used.

CCP_RDC

This class provides information on messages sent between standby and active VPMs.

CCP_RMD

This class provides information about the Received Message Distribution (RMD) class. It includes information related to the routing of IP packets (IP, UDP, ARP, ICMP, and so on).

CCP_RTD

This class contains information related to the Run Time Diagnostics (RTD) task. This task reports information on hardware presence, failure, temperature sensors and memory usage.

CCP_RTOS

This class contains information related to the Real Time Operating System. It includes information on hash and crc functions.

CCP_SC

This class contains information related to the System Control (SC) task. The SC task controls the main state of the card. It coordinates all the tasks in the arbitration process.

CCP_SCTP

This class provides information about SCTP layer events from the IUA stack.

CCP_SNMP

This class provides information relating to SNMP tasks, including SNMP health, SNMP message and trap processing.

CCP_SNMPAUD

This turns audit messages due to configuration changes made via SNMP (e.g. NetConductor) off (0) or on (1).

CCP_SYSLOG

This class contains information about the Syslog (Sl) task. It provides low-level information of the Syslog inter-workings.

CCP_TDM

This class contains information related to the TDM task. It includes information about NetRefs signalling, and TDM statistics (e.g. DS3/STM-1/OC-3/DS1/E1).

CCP_TFTP

This class contains information relating to the TFTP task. It reports the progress and status of receiving code via TFTP and the storing of it into flash.

CCP_TUCL

This class provides information about TUCL (TCP/UDP Convergence Layer) layer events from the IUA stack.

CCP_WDOG

This class provides information related to the Watchdog (WDOG) task which monitors the low-level health of the system.

CCP_XD_MEM

This class provides information related to allocating and de-allocating memory.

CCP_XUA

This class provides information on the top level control of and interaction with the IUA stack.

CCP_XUAAPI

Not currently used.

DSP Classes

This section provides a short description of each DSP class. It gives you an idea of the kind of information that can selectively be generated on command. You can turn these classes on or off as you need them.

DSP classes can be further customized using an ifIndex. The ifIndex is a parameter that specifies the endpoint (or group of endpoints; for example, DS3, DS1, or DS0). For more information on configuring the ifIndex see "Configuring Debug classes" on page 193.

DSP_CHAPI

This is the channel API module. This module provides the interface between the SYSCTL module and the VFAPI module. High level channel control is performed here including all the subscriber state machines (for example, FGD-MO, MT, ISUP), audio state machines (ringback, DTMF outpulse), and dialing state machines (inbound dialing).

DSP_CMD

This module is where the DSP side of the DSPAPI is implemented. It is responsible for sending and receiving all commands to and from the VPM.

DSP_KERNEL

This class pertains to the DSP module that contains the operating system, task scheduler, and drivers. When general system performance information is desired, this is the module of interest.

DSP_SYSCTL

This class contains the system state machine and xGCP stack. All xGCP debug information is contained here.

DSP_VFAPI

This is the voice/fax API module. This module provides a high level interface to all the main DSP functions such as voice compression, fax relay, DTMF/tone detection, VAD, LPR, echo cancellation, jitter buffer, and so on. Basically everything that relates to the actual media processing takes place here.

NP Classes

This section provides a short description the NP class. It gives you an idea of the kind of information that can selectively be generated on command. You can turn these classes on or off as you need them.

NP_GEN

This class provides information on configuration of the packet interface and messages between the NP and VPM.

B

OC3 (SONET) DS1 AND STM-1 (SDH) VC12/E1 MAPPING

This appendix covers the mapping of DS1s to OC3 (SONET) and VC12/E1 to STM-1 (SDH). It is broken into two sections:

- "DS1 to OC3 (SONET) Mapping" on page 219
- "VC12/E1 to STM-1 (SDH) Mapping" on page 220

DS1 to OC3 (SONET) Mapping

The BTX-4K follows BellCore GR-253-CORE Issue 4 for mapping DS1s into an OC3. Table 2 describes this mapping.

Table 2: DS1 to OC3 (SONET) Mapping

DS1#	STS-1	VT-Group	VT1.5	DS1#	STS-1	VT-Group	VT1.5	DS1#	STS-1	VT-Group	VT1.5
1	1	1	1	**29**	2	1	1	**57**	3	1	1
2	1	2	1	**30**	2	2	1	**58**	3	2	1
3	1	3	1	**31**	2	3	1	**59**	3	3	1
4	1	4	1	**32**	2	4	1	**60**	3	4	1
5	1	5	1	**33**	2	5	1	**61**	3	5	1
6	1	6	1	**34**	2	6	1	**62**	3	6	1
7	1	7	1	**35**	2	7	1	**63**	3	7	1
8	1	1	2	**36**	2	1	2	**64**	3	1	2
9	1	2	2	**37**	2	2	2	**65**	3	2	2
10	1	3	2	**38**	2	3	2	**66**	3	3	2
11	1	4	2	**39**	2	4	2	**67**	3	4	2
12	1	5	2	**40**	2	5	2	**68**	3	5	2
13	1	6	2	**41**	2	6	2	**69**	3	6	2
14	1	7	2	**42**	2	7	2	**70**	3	7	2
15	1	1	3	**43**	2	1	3	**71**	3	1	3
16	1	2	3	**44**	2	2	3	**72**	3	2	3
17	1	3	3	**45**	2	3	3	**73**	3	3	3
18	1	4	3	**46**	2	4	3	**74**	3	4	3
19	1	5	3	**47**	2	5	3	**75**	3	5	3
20	1	6	3	**48**	2	6	3	**76**	3	6	3
21	1	7	3	**49**	2	7	3	**77**	3	7	3
22	1	1	4	**50**	2	1	4	**78**	3	1	4
23	1	2	4	**51**	2	2	4	**79**	3	2	4
24	1	3	4	**52**	2	3	4	**80**	3	3	4
25	1	4	4	**53**	2	4	4	**81**	3	4	4
26	1	5	4	**54**	2	5	4	**82**	3	5	4
27	1	6	4	**55**	2	6	4	**83**	3	6	4
28	1	7	4	**56**	2	7	4	**84**	3	7	4

VC12/E1 to STM-1 (SDH) Mapping

The BTX-4K follows the ITU-T Recommendation G.707 for mapping VC-12s into a VC4. Table 3 describes this mapping.

Table 3: VC12/E1 to STM-1 (SDH) Mapping

TU# (VC-12/E1#)	TUG3 (K)	TUG2 (L)	TU12 (M)	TU# (VC-12/E1#)	TUG3 (K)	TUG2 (L)	TU12 (M)	TU# (VC-12/E1#)	TUG3 (K)	TUG2 (L)	TU12 (M)
1	1	1	1	**22**	1	1	2	**43**	1	1	3
2	2	1	1	**23**	2	1	2	**44**	2	1	3
3	3	1	1	**24**	3	1	2	**45**	3	1	3
4	1	2	1	**25**	1	2	2	**46**	1	2	3
5	2	2	1	**26**	2	2	2	**47**	2	2	3
6	3	2	1	**27**	3	2	2	**48**	3	2	3
7	1	3	1	**28**	1	3	2	**49**	1	3	3
8	2	3	1	**29**	2	3	2	**50**	2	3	3
9	3	3	1	**30**	3	3	2	**51**	3	3	3
10	1	4	1	**31**	1	4	2	**52**	1	4	3
11	2	4	1	**32**	2	4	2	**53**	2	4	3
12	3	4	1	**33**	3	4	2	**54**	3	4	3
13	1	5	1	**34**	1	5	2	**55**	1	5	3
14	2	5	1	**35**	2	5	2	**56**	2	5	3
15	3	5	1	**36**	3	5	2	**57**	3	5	3
16	1	6	1	**37**	1	6	2	**58**	1	6	3
17	2	6	1	**38**	2	6	2	**59**	2	6	3
18	3	6	1	**39**	3	6	2	**60**	3	6	3
19	1	7	1	**40**	1	7	2	**61**	1	7	3
20	2	7	1	**41**	2	7	2	**62**	2	7	3
21	3	7	1	**42**	3	7	2	**63**	3	7	3

GLOSSARY

Baud rate

The baud rate is a measure of the number of symbols transmitted per time unit. Each symbol consists of a number of bits, so the baud rate is only the same as the bit rate, when there is one bit per symbol.

BCM

Nuera definition that means BITS clock module. The module supports the BITS clock connection, and the 100BT and craft interface.

BITS clock

Building Integrated Timing Supply clock. The BITS clock provides a pulse that synchronizes the whole network.

BNC

Bayonet-Neill-Concelman, British Navy Connector, or Baby Nevel Connector, all coaxial cables.

CIC

Carrier Identification Code

DNS

Domain Name Server

DS0

Digital Service, level 0. DS0 is 64,000 bps, the worldwide standard speed for digitizing one voice conversation using pulse code modulation and sampling the voice

8,000 times a second and encoding the result in an 8-bit code (thus 8,000 * 8 = 64,000). There are 24 DS0 channels in a DS1.

DS1

DS1 can occur in 2 varieties, T1 or E1. T1 is commonly used in North America to multiplex 24 DS0 channels. Each DS0 channel, originally a digitized voice-grade telephone signal, carries 8000 bytes per second (64,000 bits per second). A DS1 frame includes one byte from each of the 24 DS0 channels and adds one framing bit, making a total of 193 bits per frame at 8000 frames per second. The result is 193*8000 = 1,544,000 bits per second.

E1 is the European version of DS1 and carries information at the rate of 2.048 Mbps with 30 bearer channels.

DS3

Digital Service, level 3. Equivalent to 28 T-1s and operates at 44.736 Mbps. Also called T-3.

DTMF

Dual Tone Multi-Frequency

E1

See DS1.

EMS

Element Management System. A generic name for the NetConductor. An element management system (EMS) manages one or more of a specific type of telecommunications network element (NE). Typically, the EMS manages the functions and capabilities within each NE but does not manage the traffic between different NEs in the network.

ESF/B8ZS

Extended Superframe Format/Bipolar 8 Zero Substitution.

Ethernet

A local area network used for connecting computers, printers, workstations, terminals, servers, and so on, within the same building or campus.

GUI

Graphical User Interface

IAD

Integrated Access Device. A consumer premises box which provides for the simultaneous Internet data access and voice calls over DSL broadband connection.

IP

Internet Protocol. The Internet Protocol is a standard describing software that keeps track of the internet work addresses for different nodes, routes outgoing messages, and recognizes incoming messages. It allows packets to traverse multiple networks on the way to its final destination.

IP Address

A unique, 32-bit identifier for a specific IP host computer on a network.

Masks

A field made up of letters or numbers and wildcard characters, used to filter data.

Media IP Address

This is the IP address of the GigE interface, located on the front of the VPM card.

MO/MT

Multi-frequency Feature Group D Operator Service/Multi-frequency Feature Group D Terminating Protocol.

MTA

Multimedia Terminal Adaptor. A consumer premises device that provides for the simultaneous Internet data access and voice calls over cable.

NCS

Network Call Signalling – this is the signalling protocol between the Call Management Server and MTAs

NEs

Network Elements (NEs) are those elements which are controlled by an EMS such as NetConductor.

NetConductor

Nuera's element management system

NETREF

NETREF parameters specify the source over which the gateway receives clocking information.

ORCA

Open Reliable Communications Architecture

PSTN

Public Switched Telephone Network

RTP

Realtime Transport Protocol

SNMP

Simple Network Management Protocol. SNMP is the most common method by which network management applications can query a management agent using a supported management information base.

TAC

Technical Assistance Center

TCP/IP

Transmission Control Protocol/Internet Protocol. A networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TDM

A technique for transmitting a number of separate data, voice, or video signals simultaneously over a high bandwidth communications medium by interleaving short bursts of each signal one after another.

TGCP

Trunking Gateway Control Protocol.

UDP

User Datagram Protocol. A protocol describing how messages reach applications programs within a destination computer.

VPM

Voice Processing Module

WAN

Wide Area Network

BIBLIOGRAPHY

This appendix provides a brief, annotated bibliography of publications that provide information relevant to the understanding of the design and management of the ORCA communications platform.

MicroMuse, Inc.

All information in the NetConductor User's Guide is Copyright © 2001 - 2004 Micromuse Inc. It is reused in this manual subject to the specific terms of Nuera's License agreement with MicroMuse to reproduce, rewrite, and distribute NetConductor online help and documentation to support the runtime operation of NetConductor-based products.